2011

When Machines are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches

David Thaw
University of Pittsburgh School of Law, dbthaw@pitt.edu

Priscilla Smith
Yale Law School - Information Society Project

Nabiha Syed
Stanford Law School Center for Internet and Society

Albert Wong
Columbia University - Law School

THE YALE LAW JOURNAL ONLINE

PRISCILLA J. SMITH, NABIHA SYED, DAVID THAW & ALBERT WONG

When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches

INTRODUCTION

Federal and state law enforcement officials throughout the nation are currently using Global Positioning System (GPS) technology for automated, prolonged surveillance without obtaining warrants. As a result, cases are proliferating in which criminal defendants are challenging law enforcement's warrantless uses of GPS surveillance technology, and courts are looking for direction from the Supreme Court. Most recently, a split has emerged between the Ninth and D.C. Circuit Courts of Appeal on the issue. In *United States v. Pineda-Moreno*,[1] the Ninth Circuit relied on *United States v. Knotts*[2]—which approved the limited use of beeper technology without a warrant—to uphold warrantless use of GPS surveillance technology.[3] However, in *United States v. Maynard*,[4] the D.C. Circuit held that warrants are required for law enforcement use of GPS tracking devices. In distinguishing *Knotts*, the D.C. Circuit pointed to the vast differences between the relatively primitive beeper technology used almost thirty years ago and the unprecedented power of GPS surveillance

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

2. 460 U.S. 276 (1983).

3. 591 F.3d at 1216-17.

4. 615 F.3d 544, 557 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011) (No. 10-1259).

technology used today.[5] The Seventh Circuit Court of Appeals[6] and various state courts[7] are similarly divided. In light of this confusion, the Supreme Court has recently agreed to review the issue, granting certiorari from the decision of the D.C. Circuit in *Maynard*[8] and leaving the *Pineda-Moreno* petition in a holding pattern. On November 8, the Supreme Court will hold oral arguments in the case, which was docketed under the new name *United States v. Jones*.[9]

The Supreme Court's Fourth Amendment doctrine, including its cases evaluating new surveillance technologies, has always been informed by one of the Amendment's animating principles: its mandate to prevent abuse of police

5. *See id.* at 556-58; *see also* United States v. Pineda-Moreno (*Pineda-Moreno II*), 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) (arguing that the warrant requirement must apply to GPS surveillance because GPS technology allows unprecedented intrusions into privacy).

6. United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011) (holding that no warrant was needed to track a suspect for sixty hours). *But see id.* at 286 (Wood, J., dissenting) (adopting the reasoning of the D.C. Circuit in *Maynard*); *cf.* United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) (acknowledging in dicta that "[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive" and expressing relief that the court did not have to decide the question in that case); *id.* at 997-98 ("[T]here is a difference . . . [between using the new technologies] on the one hand and following suspects around in a car on the other. The new technologies enable, as the old (because of expense) do not, wholesale surveillance.").

7. High courts in three states—Massachusetts, New York, and Washington—have held that warrants are required for the use of GPS surveillance under the state's constitution. Commonwealth v. Connolly, 913 N.E.2d 356, 366-67 (Mass. 2009); People v. Weaver, 909 N.E.2d 1195, 1201-03 (N.Y. 2009); State v. Jackson, 76 P.3d 217, 264 (Wash. 2003) (en banc). On the other hand, three state intermediate appellate courts—in Maryland, Virginia, and Wisconsin—have held that a warrant is not required for the use of GPS surveillance. Stone v. State, 941 A.2d 1238, 1250-51 (Md. Ct. Spec. App. 2008) (holding that "the appellant did not have a reasonable expectation of privacy in his location . . . in a vehicle riding on public roads, and therefore evidence about the use of the GPS device . . . was not relevant to the appellant's Fourth Amendment-based suppression motion"); Foltz v. Commonwealth, 698 S.E.2d 281, 291 n.12 (Va. Ct. App. 2010) (holding that no warrant is required for the use of GPS surveillance for under six days), *aff'd on re'h en banc*, 706 S.E.2d 914 (Va. Ct. App. 2011); State v. Sveum, 769 N.W.2d 53, 60 (Wis. Ct. App. 2009) (holding that no warrant is required for the use of GPS technology in law enforcement surveillance as long as the device is attached while the vehicle is parked in a public place), *aff'd on other grounds*, 787 N.W.2d 317 (Wis. 2010).

8. *Jones*, 131 S. Ct. at 3064.

9. *Preview of United States Supreme Court Cases:* United States v. Jones, AM. BAR ASS'N, http://www.americanbar.org/publications/preview_home/10-1259.html (last visited Oct. 11, 2011).

power.[10] While the Court has not always articulated this theory of the Fourth Amendment as clearly as it could have, a careful review of the case law reveals a concern about abuse and "a too permeating police surveillance."[11] This reading demands that, in any review of new surveillance technology, courts must evaluate the technology's potential for abuse.[12]

Unfortunately, in drawing lines between technology such as powerful binoculars that merely enhance the senses of law enforcement officials and technology such as thermal imaging devices that create new superhuman powers, the Justices have offered confusing guidance to lower courts. At times, they have relied on a distinction between sense enhancement and sense creation, a superficial distinction that fails to delineate when new surveillance technology is problematic.[13] At other times, the Court has reverted to language reminiscent of past Fourth Amendment doctrine requiring some sort of physical trespass in order to trigger the warrant requirement. The Court rejected that doctrine in *Katz v. United States*,[14] when it recognized that new technologies make a private space/public space line unworkable. However, the

10. For an interpretation of the Fourth Amendment that emphasizes its function as a check on executive power, see Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325 (2002). Ku marshals historical evidence from the seventeenth century to support the claim that "the Fourth Amendment was adopted as a means of restraining official discretion." *Id.* at 1334. As discussed below, this structural theory of the Fourth Amendment may offer more robust support for the defendants' claims in *Jones* and *Pineda-Moreno* than a notion of the Fourth Amendment focused primarily on personal privacy. *See* discussion *infra* Part I.

11. United States v. Di Re, 332 U.S. 581, 595 (1948).

12. As Daniel Solove notes, outright abuse is not the only threat posed by government information gathering: "even if government entities are not attempting to engage in social control, their activities can have collateral effects that harm democracy and self-determination." Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1101-02 (2002). The government's *capacity* to monitor the movements of millions of individuals without a warrant may produce pernicious chilling effects even if the government never exercises this capacity. *Cf. id.* at 1107 ("[O]ne need not fear the rise of a totalitarian state or the inhibition of democratic activities to desire strong controls on the power of the government in collecting personal information."). Hence this Essay focuses on the *potential* for abuse, which insulates our argument from the claim that "[l]aw enforcement *has not* abused GPS technology" and that "[n]o evidence exists of widespread, suspicionless GPS monitoring." Brief for the United States at 14, United States v. Jones, No. 10-1259 (U.S. Aug. 11, 2011), *available at* http://volokh.com/wp/wp-content/uploads/2011/08/DOJJonesBrief.pdf. *But see infra* Section II.C (suggesting evidence of abuse).

13. *See generally* David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563 (1990) (analyzing the case law of sense-enhanced searches and arguing that the Fourth Amendment can effectively regulate such searches).

14. 389 U.S. 347, 361 (1967).

Justices' failure to explain clearly the source of their concerns about new technology, coupled with their haphazard use of language, has confused the lower courts and commentators. This confusion has led some to conclude that the use of GPS surveillance technology for prolonged, automated surveillance of targets should not be considered a "search" subject to the Fourth Amendment, at least to the extent that the surveillance occurs on public streets.

As we argue in this Essay, the use of GPS surveillance for prolonged monitoring without a warrant cannot pass muster under the Fourth Amendment. It may seem at first glance that GPS tracking of public actions—actions that the police can otherwise follow without a warrant in the status quo—is harmless from a privacy perspective. After all, if cops can tail a suspect for days or weeks without a warrant, what difference does it make if the tracking is done by an undercover officer or a GPS device under the hood of a suspect's car? However, when "machines are watching"—that is, when tracking is automated and extended for prolonged periods of time—the potential for abuse grows larger. In such circumstances, the warrant requirement, with its limited exceptions, provides a necessary check on overreach by law enforcement authorities.

This Essay is organized in three Parts. In Part I, we outline the Fourth Amendment's structural protections against law enforcement abuse and explain the Court's historic approach to new surveillance technologies. While the Court's approach is undertheorized, we show that the Court has carefully examined new technologies to prevent technological end-runs around existing legal doctrine that seeks to protect personal privacy. We maintain that the Court's doctrinal distinction between sense-enhancing and sense-creating technology is effectively a proxy for the Court's underlying interest in protecting against governmental abuse.[15] In Part II, we explain why GPS surveillance technology creates unprecedented potential for abuse, and we present anecdotal evidence suggesting that abuse of GPS surveillance technology may be occurring already. Note, though, that our argument does *not* hinge on the claim that abuse is widespread. Rather, we argue that GPS surveillance poses a real threat, even if (and we have no way of knowing whether this is true) the potential for abuse has not yet been realized except in a limited number of cases. Our conception of the Fourth Amendment differs

15. Other scholars have noted the importance this distinction has played in Fourth Amendment cases. *See, e.g.*, Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 432 (2007) ("[T]he Court has, in large part, tied the scope of Fourth Amendment protection to the categorization of a technology as either sense augmenting or extrasensory."). However, none have connected the distinction to the Court's broad theory of the Fourth Amendment as protecting against governmental abuse.

fundamentally from the Solicitor General's view, expressed in the government's brief in *Jones*, that "[t]he decision whether to apply different constitutional principles to hypothetical programs of mass, suspicionless surveillance can await resolution if such programs ever occur."[16] We do not believe that the Court must stand aside until "Big Brother" arrives; doing so would render the Fourth Amendment's protections a "dead letter."[17]

In Part III, we connect our interpretation of the Fourth Amendment to the "reasonable expectation of privacy" language that looms large in contemporary case law. In our view, a "reasonable expectation of privacy" may be violated even if individuals already anticipate that the information at issue can be accessed by law enforcement officials. Indeed, any other interpretation of that language would yield perverse implications: if "hypothetical programs of mass, suspicionless surveillance" ever arrived, individuals would then have *no* expectation of privacy once they learned of the surveillance, and the "expectation of privacy" protection—if interpreted literally—would become a nullity.

Our interpretation of the Fourth Amendment is consistent with the concerns underlying past Supreme Court decisions. As Part III explains, control over information about our location is still central to our sense of self. This interpretation of the Fourth Amendment and the individual rights interpretation ultimately converge in GPS cases, and both views counsel in favor of the conclusion that the use of this technology for automated, prolonged surveillance should be subject to the Fourth Amendment's warrant requirement.

I. THE FOURTH AMENDMENT AND TECHNOLOGICAL ADVANCES

Most legal commentary on the Fourth Amendment implications of GPS surveillance technology has bypassed the core, structural Fourth Amendment issue. For example, Orin Kerr has distinguished between "public location information obtained from GPS devices" and "private facts" that fall within the ambit of the Fourth Amendment's protections.[18] In this Essay, we argue that

16. Brief for the United States, *supra* note 12, at 35.

17. Samson v. California, 547 U.S. 843, 865 n.6 (2006); *see id.* ("If high crime rates were grounds enough for disposing of Fourth Amendment protections, the Amendment long ago would have become a dead letter.").

18. For Kerr's perspective on GPS surveillance specifically, see Orin Kerr, *Does the Fourth Amendment Prohibit Warrantless GPS Surveillance?*, VOLOKH CONSPIRACY (Dec. 13, 2009, 9:46 PM), http://volokh.com/2009/12/13/does-the-fourth-amendment-prohibit-warrantless-gps-surveillance [hereinafter Kerr, *GPS Surveillance*], in which Kerr argues

the scholarly focus on the information collected by new technology[19] gives short shrift to the animating and long-honored principle of the Fourth Amendment: protection of the populace from abuse of law enforcement powers. This fundamental principle underlies the Court's decisions evaluating the application of the Fourth Amendment to the use of new surveillance technologies, including its recent decision requiring a warrant for thermal imaging in *Kyllo v. United States*.[20] In cases from *Katz* to *Knotts* to *Kyllo*, wherever a new technology carries the potential for police abuse, the Court has allowed its use only as guarded by the warrant requirement, placing a check on the unlimited discretion otherwise afforded officers. As the Supreme Court has acknowledged, "[r]equiring a warrant will have the salutary effect of ensuring that use of [new technology] is not abused."[21]

Given the Court's command to examine the reasonableness of an expectation of privacy in determining whether a search has occurred,[22] it is perhaps not surprising that commentators have focused on the nature of the information collected. And we do not mean to say that the nature of the information collected by a technology is irrelevant. If a technology only had the capacity to collect, store, and analyze data in which individuals had no privacy or dignitary interest—such as the information individuals make available to the public in phone books—then neither the abuse of that technology nor the potential for abuse would be of such grave concern. However, as the Court has repeatedly recognized, the *means* of surveillance, the nature of the technology at issue, and its potential for abuse must be considered as well.[23] Considering these three factors will impact the Court's analysis of privacy expectations, as

that a warrant is not required for GPS surveillance because there is no privacy interest in public whereabouts. On the "private facts" model more broadly, see Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 506 (2007) [hereinafter Kerr, *Four Models*].

19. Hutchins, for example, recognizes the Court's distinction between sense-augmenting and "extrasensory" technologies, *see* Hutchins, *supra* note 15, at 436, but argues that this distinction is superficial and that the key inquiry lies in the information obtained by the technology, *id.* at 437-38. *See also* Kerr, *GPS Surveillance*, *supra* note 18 (arguing that "the key question is the nature of the information collected instead of the details of the technology used to collect it").

20. 533 U.S. 27 (2001).

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

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

23. *Kyllo*, 533 U.S. at 37-39; Whalen v. Roe, 429 U.S. 589, 606-07 (1977) (Brennan, J., concurring) (asserting that the Fourth Amendment limits not only "the type of information the State may gather but also . . . the means it may use to gather it"); Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.").

we outline in Part III below. We start, however, with an examination of how the Court has treated the potential for law enforcement abuse of surveillance methods in the past.

A. The Fourth Amendment's Emphasis on Law Enforcement Abuse

As has been thoroughly documented, the Founders designed the Fourth Amendment to protect citizens against arbitrary police invasions,[24] a direct response to unwarranted searches and seizures by British officers targeting political opponents both in England and in the colonies.[25] As the Court cautioned more than eighty years ago, "[t]he Fourth Amendment was adopted in view of long misuse of power in the matter of searches and seizures both in England and the colonies."[26] The Court sees the Amendment playing a robust role as our primary protection against "a too permeating police surveillance."[27] And it is the warrant requirement that is the Court's means of enforcing this protection.[28]

In addition to protecting personal space from invasion, thereby protecting our homes as our castles, the Fourth Amendment also serves a crucial function in preserving an open democratic process and in ensuring the equal treatment of citizens.[29] It stops police from using surveillance to intimidate targeted groups of citizens and prevent their free and equal participation in political organization and discussion.[30] Moreover, the Fourth Amendment's protections reflect the view that certain individuals are more at risk than others when they gather to discuss politics, transact business, or even seek medical care.[31] To

24. *See* Camara v. Mun. Court, 387 U.S. 523, 528 (1967).

25. *See* Payton v. New York, 445 U.S. 573, 583 & n.21 (1980).

26. Byars v. United States, 273 U.S. 28, 33-34 (1927).

27. United States v. Di Re, 332 U.S. 581, 595 (1948).

28. *See* Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring) ("As elsewhere under the Fourth Amendment, warrants are the general rule, to which the legitimate needs of law enforcement may demand specific exceptions.").

29. *See generally* Solove, *supra* note 12, at 1122 ("[T]he Fourth Amendment provides for an architecture of power, a structure of protection that safeguards a range of different social practices of which privacy forms an integral dimension.").

30. *See, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 225 (1973) (recognizing that "the possibility of unfair and even brutal police tactics poses a real and serious threat to civilized notions of justice").

31. *See generally* Ferguson v. City of Charleston, 531 U.S. 67, 70-73 (2001) (describing a policy developed by a public hospital in collusion with police and prosecutors to test for drugs in pregnant women in the public hospital but not in private hospitals).

protect against abuse of "discretion," the Fourth Amendment requires that "the usual inferences which reasonable men draw from evidence . . . be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."[32] The Court itself has indicated that the warrant requirement and the exclusionary rule are the only effective limitations on lawless searches and seizures.[33]

B. New Technologies and the Fourth Amendment

When examining the use of new surveillance technologies, the Court has recognized that old Fourth Amendment legal standards may not provide enough protection because a new technology can create powers of surveillance that were not anticipated when old legal standards were developed. The Court therefore discourages the "mechanical" application of doctrinal standards that allow end-runs around Fourth Amendment protections and leave us "at the mercy of advancing technology."[34] Instead, the Court encourages the adoption of rules that "take account of more sophisticated systems that are already in use or in development."[35] Any standard applied must meet the broader structural concerns of the Fourth Amendment and "assure[the] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[36]

In its decisions examining whether law enforcement use of a new surveillance method should be allowed without the minimal limitations of a warrant, the Court has not hesitated to modify its Fourth Amendment inquiry as necessary to ensure that the purpose underlying the Amendment is carried forward. For example, in *Katz*,[37] the Court evaluated law enforcement's use of a novel listening device, one that attached to the *outside* of phone booths but nevertheless allowed police officers to eavesdrop on a target's phone conversations. This method met the technical requirements of Fourth

32. Payton v. New York, 445 U.S. 573, 586 n.24 (1980) (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).

33. *See* Elkins v. United States, 364 U.S. 206, 220 (1960) ("[N]either administrative, criminal nor civil remedies are effective in suppressing lawless searches and seizures." (citing People v. Cahan, 282 P.2d 905, 913 (Cal. 1955))). *But see* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 812-16 (1994) (arguing that revitalized civil remedies would be sufficient to control police abuse).

34. Kyllo v. United States, 533 U.S. 27, 35 (2001).

35. *Id.* at 36.

36. *Id.* at 34.

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

Amendment doctrine at the time, which only prohibited *physical* intrusions into the private sphere.[38] Nevertheless, the Court modified the doctrine to fit new realities, recognizing that the difference between physical and electronic intrusion had "no constitutional significance."[39] The Court held that the Fourth Amendment protects "people, not places"[40] and emphasized that notions of privacy and improper intrusion cannot be defeated by technological end-runs around previous doctrine.[41]

The Court's concern about limiting police discretion, police abuse, and the extent to which we become a surveillance state has also been expressed in its cases distinguishing sense-enhancing from sense-creating technologies. Under this line of reasoning, the Court has required a warrant for technologies that do not enhance human senses but operate independently of humans. While the sense enhancement/sense creation doctrine provides some direction to lower courts, reliance on the doctrine is problematic in light of the difficulty in knowing when sense enhancement has crossed the line into sense creation. At other times, the Court has confused the issue by reverting to language reminiscent of the pre-*Katz*, private space/public space distinction. We submit, however, that none of the cases turn on either of these distinctions. The Court's decisions are instead animated by the abuse potential of each surveillance technology.

For example, in *United States v. Lee*,[42] the Court confirmed that no search took place where officers used "searchlights" or "marine glass or field glass" to help them see on the deck of a ship at night.[43] This limited form of sense enhancement did not implicate protections against police abuse any more than what an individual officer watching without binoculars would have done. In contrast, in *Walter v. United States*,[44] the Court held that using a movie projector—fairly basic technology, even at the time—to view films without a warrant was an unreasonable search under the Fourth Amendment. In *Walter*, the government argued that agents did not need a warrant to view the films

38. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

39. *Katz*, 389 U.S. at 353.

40. *Id*. at 351.

41. *See id.* at 362 (Harlan, J., concurring). The protections of the Fourth Amendment go beyond the walls of each man's "castle." *See, e.g.*, Stanley v. Georgia, 394 U.S. 557, 564 (1969) (noting that the Founders also "protect[ed] Americans in their beliefs, their thoughts, their emotions and their sensations" (quoting *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting))).

42. 274 U.S. 559 (1927).

43. *Id.* at 563.

44. 447 U.S. 649 (1980).

because they were lawfully in possession of the materials. The Court rejected that argument, pointing out the potential for abuse if agents could open sealed letters that were lawfully in the Postal Service's possession.[45] Underlying the Court's decision was a desire to provide constitutional protection to unpopular messages.[46]

The Court's decision in *Knotts*, which upheld the limited use of beepers without a warrant, purports to rest on the sense enhancement/sense creation distinction.[47] Referencing the searchlights and marine and field glass at issue in *Lee*, the Court explained 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."[48] Yet the language of "sense enhancement" here is mystifying: it is not at all clear what "sense" the beepers "enhanced." Unlike searchlights or binoculars, the beepers in *Knotts* did not merely make it easier for the officers to "see." Indeed, the Court recognized that, but for the beepers, the police would have been unable to ascertain the suspect's location.[49] It seems therefore that the rationale underlying *Knotts* was not the sense enhancement/sense creation distinction, but rather the view of the Court that primitive beeper technology was not susceptible to abuse. After all, the *Knotts* Court specifically reserved the question of technology giving broader surveillance powers and declined to predict the outcome of a case in which technology allowed for "dragnet-type law enforcement."[50] *United States v. Karo*,[51] decided one year later, makes clear the limitations of the *Knotts* decision. The Court held that a warrant *was* required for monitoring and downloading beeper data when the beeper allowed surveillance of areas that officers would not otherwise have been able to view.[52]

45. *Id.* at 655.

46. *See id.*

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

48. *Id.* at 282.

49. *Id.* at 285 ("Admittedly, because of the failure of the visual surveillance, the beeper enabled the law enforcement officials in this case to ascertain the ultimate resting place of the chloroform when they would not have been able to do so had they relied solely on their naked eyes.").

50. *Id.* at 283-84; *see also* United States v. Maynard, 615 F.3d 544, 556 (D.C. Cir. 2010) ("[T]he [*Knotts*] Court specifically reserved the question whether a warrant would be required in a case involving 'twenty-four hour surveillance' . . . ." (quoting *Knotts*, 460 U.S. at 283)), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011) (No. 10-1259).

51. 468 U.S. 705 (1984).

52. *Id.* at 714.

The Court's most recent discussion of these issues in *Kyllo v. United States*, which examined the application of the warrant rule to the use of thermal imaging technology, highlights how the Justices consider the abuse potential of a surveillance technology.[53] The Court began by recognizing that it had "previously reserved judgment as to how much technological enhancement of ordinary perception . . . , if any, is too much."[54] Even while recognizing the thermal imaging technology at issue to be "relatively crude," the Court in *Kyllo* advocated adopting a rule that would "take account of more sophisticated systems that are already in use or in development."[55] At some point, the Court warned, technology might advance to the point where law enforcement could see through walls.[56] Thus, even with the crude technology at issue in *Kyllo*, the potential for abuse was vast. In rejecting the government's argument that only "intimate details" should be protected, the Court pointed out that the device might be able to reveal at what hour the lady of the house takes her nightly bath.[57] Advanced forms of the technology—used without a warrant—would almost certainly "shrink the realm of guaranteed privacy."[58] While the Court was nominally protecting the "sanctity of the home,"[59] the underlying rationale for *Kyllo*—as with the other surveillance cases—is the need to protect against police abuse. Thus the Court's decision about whether a warrant is required turns on its structural concern about the potential for abuse.

C. The Ninth Circuit's Error

The true distinction between *Kyllo* (warrant required) and *Knotts* (warrant not required), expressed subtly by the Court, eluded the Ninth Circuit. That court suggested that the thermal imaging technology in *Kyllo* triggered the Fourth Amendment because thermal imaging gathered information that otherwise would have been obtained only by "a search unequivocally within the meaning of the Fourth Amendment,"[60]—i.e., a search of the home. However, that logic is flawed. The officers in *Kyllo* could have discovered the

53. 533 U.S. 27 (2001).

54. *Id.* at 33.

55. *Id.* at 36.

56. *Id.* at 36 n.3.

57. *Id.* at 38.

58. *Id.* at 34.

59. *Id.*

60. *Pineda-Moreno I*, 591 F.3d 1212, 1216 (9th Cir.), *reh'g en banc denied*, 617 F.3d 1120 (9th Cir. 2010).

evidence by looking into the home from the outside with binoculars, and such surveillance would have been allowable without a warrant.[61] The relevant distinction in *Kyllo* therefore must not be between evidence discovered indoors or outdoors but rather must be the Court's discomfort with the use of a technology that showed vast abuse potential. With such superhero X-ray vision, walls were no longer a barrier against governmental surveillance. The Fourth Amendment's Framers assumed certain physical "checks and balances" on governmental monitoring—e.g., that walls would not be transparent and that one officer would not be able to tail two different suspects in two different locations at one single moment. Where technological change has broken down these limitations, the Court has sought to restore them. This is the fundamental distinction between *Knotts* on the one hand and *Kyllo*, *Katz*, and *Walter* on the other. The Ninth Circuit ignored this important distinction and relied on *Knotts*,[62] despite the government's "limited use" of signals from the beeper.[63]

In reaching its decision, the Ninth Circuit wrote off the Supreme Court's concern about the potential for mass surveillance. According to Judge O'Scannlain, quoting the Seventh Circuit: "[s]hould [the] government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search."[64] It is important to note, though, that there is nothing in the Ninth Circuit's decision that would prevent "mass" surveillance. Imagine that law enforcement officials were engaged in mass surveillance of, for example, every person with a Latino surname who purchases fertilizer. One would need to adopt an extraordinarily impoverished view of the Fourth Amendment in order to consider this constitutionally permissible. But under the Ninth Circuit's decision in *Pineda-Moreno*, law enforcement officials "conducted no search, and Pineda-Moreno

61. The *Kyllo* Court rejected as "quite irrelevant" the dissent's objection that heat emanating from the home can sometimes be perceived by observers without the use of technology. *Kyllo*, 533 U.S. at 35 n.2; *see also id.* ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.").

62. *Pineda-Moreno I*, 591 F.3d at 1216.

63. United States v. Knotts, 460 U.S. 276, 284 (1983); *id.* at 284-85 (holding that the beeper signal was not received or relied on after the container ended the journey during which it was tracked by a law enforcement officer); *see also Pineda-Moreno II*, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) (contrasting types of surveillance).

64. *Pineda-Moreno I*, 591 F.3d at 1217 n.2 (quoting United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) (alterations in original)).

can assert no Fourth Amendment violation,"[65] no matter how unreasonable the "non-search" might have been.

II. THE UNIQUE CAPABILITIES OF GPS TECHNOLOGY

Once the source of the Court's discomfort with new technologies is properly identified as a concern about law enforcement abuse, the problem with GPS surveillance technology becomes somewhat clearer. There is a vast technical valley between old technologies used by police officers, which merely assist in tailing suspects, and modern GPS surveillance technology, which automates tracking and surveillance. The unique capabilities of these automated systems, which turn over the surveillance function to machines, are constitutionally significant because they vastly increase the likelihood of abuse. In this Part, we describe how GPS surveillance technology works and demonstrate how its technical details create enormous potential for abuse.

A. GPS Surveillance Technology Operates Independently of Humans

Modern GPS surveillance technology is a satellite-based service consisting of three parts. First, a GPS receiver (the "tracking device"), which is generally minuscule and inexpensive, autonomously calculates latitude, longitude, altitude, direction, and speed by receiving and processing location information from the transmissions of at least four GPS satellites in nearby orbit. The average case location capabilities specified in the current (2008) GPS standard call for better than nine meters horizontal accuracy and better than fifteen meters vertical accuracy.[66] The Nationwide Differential GPS (NDGPS) system enhancement enables an average location accuracy of one to three meters for compatible receivers and provides coverage over approximately ninety-two percent of the contiguous forty-eight states.[67] Further improvement efforts

65. *Id.* at 1215.

66. U.S. DEP'T OF DEF., GLOBAL POSITIONING SYSTEM STANDARD POSITIONING SERVICE PERFORMANCE STANDARD 34 (4th ed. 2008), *available at* http://www.pnt.gov/public/docs/2008/spsps2008.pdf.

67. ARINC INC., NDGPS ASSESSMENT FINAL REPORT, at ES-8 (2008), *available at* http://www.navcen.uscg.gov/pdf/ndgps/ndgps%20assessment%20report_final.pdf (noting that "NDGPS provides 1 to 3 meter horizontal accuracy (at 95% confidence) or better" and that the "NDGPS service is free and available to anyone with an NDGPS receiver"); Research & Innovative Tech. Admin., *Report to Congress: Recapitalization Plan for the Nationwide Differential Global Positioning System (NDGPS)*, U.S. DEP'T OF TRANSP. (June 2010), *available at* http://ntl.bts.gov/lib/34000/34800/34831/NDGPS_Report_to_Congress_--_FINAL_as_Signed_072010.pdf (explaining that terrestrial NDGPS in the United States is operated by

underway seek to achieve within ten centimeters horizontal accuracy and twenty centimeters vertical accuracy.[68] Second, a wireless transmitter attached to the tracking device sends the calculated location information to a specified remote destination. Finally, a law enforcement computer records the transmitted tracking data, stores it for an unlimited amount of time, and compares it with data collected from other targets.[69] The first item comprises the "core" location-determining technology used in GPS surveillance; the second and third items are technologies to collect and process that location information for law enforcement use. Alternate methods of retrieving this information exist. Some GPS tracking devices can store the information internally. Officers can then manually retrieve the data, or they can do so remotely—by triggering short-duration (or "burst") wireless transmissions—when they are within the device's range.[70]

Accordingly, electronic systems such as beeper devices used in the 1980s are simple tools when compared with modern GPS surveillance technology. As described by the Supreme Court in *Knotts*, "[a] beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver."[71] After receiving the signal, the strength of which indicates whether the object to which the beeper is attached is approaching or moving away, police officers *in the vicinity* could use this information to respond accordingly.[72] Beepers could neither determine the location themselves nor store that data.[73] The beepers in *Knotts* are thus not at all analogous to GPS technology.

the U.S. Coast Guard under a 1999 Memorandum of Agreement with the U.S. Department of Transportation and also that "the combined 87 sites provide 92 percent of the contiguous 48 states with single signal coverage").

68. ARINC INC., *supra* note 67, at ES-3 (explaining that "[t]he High Accuracy NDGPS (HA-NDGPS) program will provide the capability to broadcast GPS observables and other data to enable the user to achieve better than 10 centimeter horizontal and 20 centimeter vertical accuracy (at 95% confidence) throughout the coverage area").

69. *See* Hutchins, *supra* note 15, at 458. *See generally Frequently Asked Questions*, GPS.GOV, http://www.gps.gov/support/faq (last updated June 6, 2011) (explaining the benefits of GPS technology).

70. For an example of a commercially manufactured burst transmission-enabled GPS unit designed for use in search-and-rescue and combat operations, see *Multi Function Personal Locator Beacons PLUS Embedded GPS: Series 500-27-07*, HR SMITH GRP. OF COS. http://www.hr-smith.com/images/stories/500-27-07.pdf (last visited Oct. 11, 2011).

71. United States v. Knotts, 460 U.S. 276, 277 (1983).

72. *Id.*

73. *Pineda-Moreno II*, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) ("If no one was close enough to pick up the signal, [the data] was lost forever.").

B. The Potential for Abuse

Two aspects of GPS surveillance technology make it prone to abuse. First, once the GPS tracking device is installed, it can operate autonomously over a prolonged period of time without human involvement, independently determining and remotely transmitting positional data twenty-four hours a day. Unlike the beepers in *Knotts*, police officers need not tail the GPS tracking device in order to determine location information. As Chief Judge Kozinski explains in his dissent from the denial of rehearing *Pineda-Moreno* en banc:

> Beepers could help police keep vehicles in view when following them, or find them when they lost sight of them, but they still required at least one officer—and usually many more—to follow the suspect. The modern devices used in Pineda-Moreno's case can record the car's movements without human intervention.[74]

The requirement that law enforcement officers actively maintain proximity to the surveillance device—a notable limitation of "beeper" and other similar transponder-based location systems—is simply not present when using GPS technology. In this way, GPS technology eliminates the constraint placed on police surveillance capabilities by the limited number of officers available at any given time to track the public's movements. In the past, it was simply impossible for the police to assign an officer to track large groups of citizens around the clock. This new technology thus advances the government's surveillance capabilities and "shrink[s] the realm of guaranteed privacy."[75] By far exceeding the human capacity for surveillance, these machines create the potential for surveillance of particular individuals, unpopular groups, and eventually the entire populace. This surveillance could remain entirely undetected.

Second, the electronic storage of gathered location data allows the data to be stored forever and considered at any time in the future alongside data collected from other citizens. In contrast to beeper data, which are lost forever unless an individual records and stores the information, GPS-associated computers can by themselves compare data gathered from different individuals

74. *Id.*

75. Kyllo v. United States, 533 U.S. 27, 34 (2001).

and identify common patterns of behavior and gatherings of groups of people.[76] As Chief Judge Kozinski commented:

> By tracking and recording the movements of millions of individuals the government can use computers to detect patterns and develop suspicions. It can also learn a great deal about us because where we go says much about who we are .... Were Jones, Aaronson and Rutherford at that protest outside the White House?[77]

GPS technology is capable of retaining information for an unlimited amount of time, making targets of tracking vulnerable to intrusive data analysis of where they went and who they saw for years after the fact.

C. Evidence of Use, Suggestions of Abuse

The precise scope of GPS surveillance is unknown; there are no nationwide statistics available on the frequency of GPS surveillance, and most police departments resist disclosing how often they use it. However, the Federal Law Enforcement Training Center has issued a special bulletin advising officers in the use of GPS technology,[78] and some local jurisdictions have willingly reported the scope of their use.[79] For example, one police department in Fairfax, Virginia reported using GPS surveillance sixty-one times in 2005 alone.[80] The ACLU and its affiliates recently filed 379 public records requests in thirty-one states to determine the scope of GPS surveillance more precisely.[81] As we await responses to those requests, accounts of GPS surveillance are

76. *Cf. Pineda-Moreno II*, 617 F.3d at 1124 (Kozinski, C.J., dissenting from denial of rehearing en banc) (distinguishing GPS systems from beeper systems on the basis that without human involvement beeper data was "lost forever").

77. *Id.* at 1125.

78. *See* Keith Hodges, *Tracking "Bad Guys": Legal Considerations in Using GPS*, FBI L. ENFORCEMENT BULL. (Fed. Bureau of Investigation, Washingon, D.C.), July 2007, at 25, *available at* http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/articles/FBI-LE-Bulletin-GPS-Tracking-Jul2007.pdf.

79. *See* Ben Hubbard, *Police Turn to Secret Weapon: GPS Device*, WASH. POST, Aug. 13, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/12/AR2008081203275.html.

80. *Id.*; *see also* Foltz v. Commonwealth, 698 S.E.2d 281, 284 n.3 (Va. Ct. App. 2010) (discussing evidence of the frequency of use by local law enforcement in a challenge to GPS surveillance).

81. *See* Allie Bohm, *Your Cell Phone Knows Where You Were Last Night ... Who Else Does?*, ACLU: BLOG RTS. (Aug. 3, 2011, 12:36 PM), http://www.aclu.org/blog/protecting-civil-liberties-digital-age/your-cell-phone-knows-where-you-were-last-night-who-else.

necessarily anecdotal. The president of the National Association of Criminal Defense Lawyers, for instance, reports that GPS surveillance has been used "in cases from New York City to small towns—whoever can afford to get the equipment and plant it on a car."[82]

In one recent incident, a twenty-year-old college student from Santa Clara, California, Yasir Afifi, discovered a GPS surveillance device affixed to his car. Afifi is an American citizen whose father, also an American citizen, was president of a Muslim community association in the United States before moving to Egypt in 2003. Forty-eight hours after Afifi removed the device and asked for help online to identify it, he received a visit from several FBI agents who demanded the return of the device. Afifi was then questioned about an online blog maintained by his close friend. To date, he has not been charged with a crime. The FBI, after reclaiming the tracking device, has provided no further details.[83]

The anecdotal evidence presented here—the Fairfax data, the FBI bulletin, the Afifi case, and so on—fall well short of the "mass, suspicionless surveillance" that the Solicitor General says might trigger a warrant requirement.[84] Yet it is worth reflecting for a moment on what circumstances might trigger such "mass, suspicionless surveillance"—e.g., a terrorist attack by enemies (either foreign or domestic) whose ethnicity, religious affiliation, political persuasion, or other characteristics catalyze fear of or animus toward a particular minority group. It seems strange to say that under *those* circumstances, courts would shift from the no-warrant default rule to a heightened standard of Fourth Amendment protection. After all, civil liberties in times of emergency are subject to a one-way ratchet, and the direction is down.[85] The rules we set now, in "normal" times, ten years after the last attack on U.S. soil, serve as a ceiling, not a floor. The Solicitor General's claim that the warrant question "can await resolution" until we see an uptick in use of GPS surveillance ignores the political economy of emergency.[86]

82. Hubbard, *supra* note 79.

83. *See* Kim Zetter, *Caught Spying on Student, FBI Demands GPS Tracker Back*, WIRED, Oct. 7, 2010, http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/all/1. Afifi recently filed a civil suit seeking damages for the intrusiveness of the GPS surveillance. Press Release, Council on American-Islamic Relations, FBI Sued for Warrantless GPS Surveillance of Calif. Muslim (Mar. 2, 2011), http://www.cair.com/ArticleDetails.aspx?mid1=777&&ArticleID=26745.

84. *See supra* note 16 and accompanying text.

85. *See* Geoffrey R. Stone, *Civil Liberties in Wartime*, 28 J. SUP. CT. HIST. 215, 215 (2003).

86. David Steinberg has argued that "the regulation of powerful new search techniques should come from statutes written by elected legislators." David E. Steinberg, *Sense-Enhanced*

III. GPS SURVEILLANCE, DIGNITY INTERESTS, AND CORE CONSTITUTIONAL RIGHTS

So far, the analysis in this Essay has not yet tackled the Supreme Court's "expectation of privacy" standard, which complicates—but ultimately strengthens—our argument. As then-Justice Rehnquist recognized in *Knotts*, "th[e] Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action."[87] In *Pineda-Moreno*, the Ninth Circuit relied on *Knotts* to hold that the government can use GPS surveillance technology without warrants because individuals have no reasonable expectation of privacy in their movements through public space.[88] But individuals *do* have a "reasonable expectation" that they are not being watched (at least not constantly), and *that* expectation is threatened by GPS surveillance, regardless of whether the expectation attaches to any particular fact on its own.

Moreover, and more importantly, a robust Fourth Amendment cannot depend on whether individuals *expect* that particular facts will be kept private. If that were the case, then in a scenario in which the government ignored privacy rights on a vast scale—as in George Orwell's *Nineteen Eighty-Four*,[89] Terry Gilliam's 1985 movie *Brazil*,[90] or the contemporary children's book *The Hunger Games*[91]—there would be *no* expectation of privacy at all. The Ninth Circuit's interpretation of the "expectation of privacy" criterion creates the paradoxical situation in which law enforcement overreach is legitimized once it becomes routinized. Surely, the Fourth Amendment is robust enough that it would not lose its force if members of the public came to think that "Big Brother" behavior on the part of police officers was par for the course.

Searches and the Irrelevance of the Fourth Amendment, 16 WM. & MARY BILL RTS. J. 465, 467 (2007). The institutional questions implicated by that claim lie beyond the scope of this Essay; the Supreme Court, for its part, has not been willing to cede this territory to the political branches. *See supra* Section I.A.

87. United States v. Knotts, 460 U.S. 276, 280 (1983) (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

88. *Pineda-Moreno I*, 591 F.3d 1212, 1216-17 (9th Cir.), *reh'g en banc denied*, 617 F.3d 1120 (9th Cir. 2010); *see also* Orin Kerr, *GPS Surveillance*, *supra* note 18 (applying *Knotts* to reach the conclusion that warrants are not required).

89. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949). While the world of Orwell's *Nineteen Eighty-Four* may be our most culturally recognizable icon of totalitarianism and as such is an overused reference point, it is no less illustrative.

90. BRAZIL (Embassy International Pictures 1985).

91. SUZANNE COLLINS, THE HUNGER GAMES (2008).

To be tenable, the "expectation of privacy" requirement must protect something more than our predictions whether a particular fact or act will lie outside the state's line of sight. The D.C. Circuit's analysis in *Maynard* seemed to grasp this need. The circuit court concluded that prolonged GPS surveillance allows the government to develop an overall picture of people's lives that goes far beyond what individuals expect others to know about their actions.[92] Our E-ZPass account records and airline reservations might reveal our comings and goings in broad brushstrokes, but GPS surveillance allows the government to see our microlevel movements: what house of worship we attend, and how often; whether we see a psychiatrist; with whom we spend the night; where we eat; where we exercise; and whether we attend a particular political organization's meetings. That this information might be discoverable through credit card records or other sources is no answer: when news broke that the FBI had accessed credit card records without a warrant, the Justice Department's Inspector General called the actions "serious misconduct."[93] By contrast, the Justice Department does not apologize for warrantless GPS surveillance; rather, it unabashedly defends the practice.

The following sections elaborate two interpretations of "expectation of privacy": one in which the expectation attaches to specific facts and acts and is dependent on the context of actions and behavior, and another in which the expectation protects a less clearly delineated sphere of personal and communal life. We contend that both understandings support Fourth Amendment protection in the GPS context, though only the latter addresses the argument, mentioned above, that a prediction-based privacy right will paradoxically grow weaker as government intrusions into the private sphere grow more severe.

A. *Expectation Depends on Context*

Taking seriously the Supreme Court's mandate that we must not allow new technology to "shrink the private realm" requires us to examine the impact that the means of surveillance, the nature of the technology at issue, and its

92. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble."), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011) (No. 10-1259).

93. Ken Dilanian, *FBI Involved in Hundreds of Violations in National Security Investigations*, L.A. TIMES, Jan. 30, 2011, http://articles.latimes.com/2011/jan/30/nation/la-na-fbi-violations-20110130.

potential for abuse will have on our privacy expectations.[94] Where technology changes what is visible and knowable about us, we cannot afford to revive the rejected Fourth Amendment doctrine that attempted to draw a strict line between public and private space based on notions of physical trespass.

As the D.C. Circuit concluded, GPS surveillance invades a reasonable expectation of privacy because prolonged surveillance from the sky allows the government to develop an overall picture of people's lives that goes far beyond what individuals expect others to know about their public actions.[95] Specifically, it is the *prolonged* nature of the surveillance that creates the problem. Prolonged use of GPS surveillance technology allows the collection of a more detailed view of a person's life and activities than that gained by short bursts of tracking,[96] both because the duration of the tracking allows the collection of more information and because GPS technology collects an unprecedented amount of detail on its target's movements.[97] This approach to evaluating whether an invasion of privacy has occurred, described by the D.C. Circuit as recognizing that "the whole is something different than the sum of its parts,"[98] is not novel.[99] Instead, it is a straightforward application of the rule that whether a law enforcement search is "reasonable" is a fact-specific inquiry that must be determined through review of "the totality of the

94. Kyllo v. United States, 533 U.S. 27, 37-39 (2001); Whalen v. Roe, 429 U.S. 589, 606-07 (1977) (Brennan, J., concurring) (asserting that the Fourth Amendment limits not only "the type of information the State may gather," but also "the means it may use to gather it"); Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.").

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

96. *Id.* at 557 ("According to the [Supreme] Court, its decision [in *Knotts*] should not be read to sanction 'twenty-four hour surveillance of any citizen of this country.'" (quoting United States v. Knotts, 460 U.S. 276, 284 (1983))).

97. *See supra* Part II.

98. *Maynard*, 615 F.3d at 561 n.4 (quoting KURT KOFFKA, PRINCIPLES OF GESTALT PSYCHOLOGY 176 (1935)); *id.* at 558 (explaining that the whole of one's movements over the course of a month "reveals more—sometimes a great deal more—than does the sum of its parts").

99. *See id.* at 562 ("What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene." (quoting CIA v. Sims, 471 U.S. 159, 178 (1985))). Orin Kerr has called the *Maynard* court's analysis a "mosaic theory." Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search. Kerr's assessment trivializes the detailed factual analysis of privacy interests required under the Supreme Court's jurisprudence and is a misnomer in any case.

circumstances."[100] Indeed, this type of analysis—rather than reliance on public versus private space—is required by *Katz*, where the Court held that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[101]

As Helen Nissenbaum points out, *where* behavior occurs is not always determinative of the private nature of that behavior; instead, "norms of appropriateness dictate what information about persons is appropriate, or fitting, to reveal in a particular context."[102] She argues:

> [W]hether a particular action is determined a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination.[103]

The Supreme Court has followed this logical approach to determining privacy expectations in another context. For example, in *Ferguson v. City of Charleston*, the Court recognized that there is a difference between handing over one's bodily fluids for drug testing in a medical context and handing over one's bodily fluids outside a medical context.[104] Because "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent,"[105] the plaintiffs in that case had an expectation of privacy in the results of drug tests of fluids they shared with medical personnel. The expectation of privacy differs based on who was given the fluids and in what context.[106]

100. *See, e.g.*, Ohio v. Robinette, 519 U.S. 33, 39 (1996).

101. Katz v. United States, 389 U.S. 347, 351 (1967); *see also* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 26-27 (2005).

102. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 138 (2004); *see also* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1145 (2002) ("[P]rivacy must be valued contextually.").

103. Nissenbaum, *supra* note 102, at 155.

104. 531 U.S. 67 (2001).

105. *Id.* at 78.

106. Similarly, in *Ohio v. Robinette*, the Supreme Court rejected a bright-line rule for determining the voluntariness of consent to a search and thus the reasonableness of the search in favor of a "traditional contextual approach." 519 U.S. 33, 39 (1996) (quoting Michigan v. Chesternut, 486 U.S. 567, 573 (1988)).

Similarly, context determines whether we expect privacy while driving on public highways—or in any public setting. As Nissenbaum argues, "[t]he notion that when individuals venture out in public . . . 'anything goes,' is pure fiction. . . . [E]ven in the most public of places, it is not out of order for people to respond in word or thought, 'none of your business,' to a stranger asking their names."[107] Michael Froomkin points out that "at least in large cities, one enjoys the illusion, and to a large extent the reality, of being able to move about with anonymity."[108] In fact, the conception of privacy as a form of total secrecy is ill-suited to the digital information age: "[t]he people we call, the papers we discard, and our financial records are commonly understood as private matters even though third-parties may have access to (or even possess) that information."[109] Ultimately, "clinging to the notion of privacy as total secrecy would mean the practical extinction of privacy in today's world."[110]

Additionally, the public's *behavior* toward encroaching forms of surveillance is relevant to whether courts can infer that the public believes certain actions are private. On this count, the American public has clearly rejected the notion that the government should be able to follow us without our consent. Although many Americans are comfortable with using a GPS service to determine their own personal location when that service operates subject to their consent and control,[111] Americans are uncomfortable with GPS surveillance technology when there is even a slight loss of user control.[112] For example, despite a strong push by companies encouraging Americans to adopt "geosocial" software that would allow users to broadcast their locations to selected friends using GPS in

107. Nissenbaum, *supra* note 102, at 139; *see also id.* at 143 (arguing that "a privacy violation has occurred when . . . contextual norms of appropriateness . . . have been breached").

108. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1476 (2000).

109. Solove, *supra* note 102, at 1152.

110. *Id.*

111. Subscription services such as OnStar can access an automobile's location and even transmit this location in case of emergency or theft, but only with the consent of the user. *See, e.g.*, *OnStar Privacy Statement*, ONSTAR, http://www.onstar.com/web/fmv/privacy (last updated Jan. 1, 2011).

112. GPS technology is also used by some private and government employers to ensure job performance and service delivery, but this use is limited to the terms of the employment relationship and happens only while the employee is on the job using a vehicle owned by the employer. *See, e.g.*, Judy Muller, *City Monitors Employees with GPS*, ABC NEWS, Feb. 21 2004, http://abcnews.go.com/WNT/story?id=129219 (explaining that city governments use GPS tracking systems to ensure efficiency and monitor services such as street sweeping and pothole fixing); *On Your Tracks: GPS Tracking in the Workplace*, NAT'L WORKRIGHTS INST. 10 (n.d.), http://workrights.us/wp-content/uploads/2011/02/NWI_GPS_Report.pdf.

their phones, only four percent of online adult Americans use these services.[113] For those skeptical whether there can be any plausible privacy expectation for these public actions, as Chief Judge Kozinski noted, "[y]ou can preserve your anonymity from prying eyes, even in public, by traveling at night, through heavy traffic, in crowds, by using a circuitous route, disguising your appearance, passing in and out of buildings and being careful not to be followed."[114] As the *Maynard* court observed, we have not become a society that expects this monitoring of our daily activities, and there is no sign that we would accept that type of oversight.[115]

Indeed, even the federal government recognizes that members of the American public do not expect to disclose data about their movements from place to place throughout the day. To recruit volunteers whose vehicles would be equipped with GPS devices for a federally funded study to assess a new mileage-based tax, study organizers felt it necessary to assure volunteers that "[n]o detailed route information regarding your driving will be stored or collected"[116] and that information about mileage would be maintained in "highly secure locations" in a separate database on a separate server from their personal information.[117] The organizers' assurances indicate their recognition of a reasonable expectation of privacy in data about public movements.

B. Privacy as Self-Definition and Dignity

When our activities and our patterns of behavior are exposed to view, our sphere of self shrinks accordingly. The expectation that these "private" matters

---

113. Kathryn Zickuhr & Aaron Smith, *4% of Online Americans Use Location-Based Services*, PEW INTERNET & AM. LIFE PROJECT (Nov. 4, 2010), http://pewinternet.org/~/media/Files/Reports/2010/PIP-Location%20based%20services.pdf.

114. *Pineda-Moreno II*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc).

115. United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) ("A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'" (quoting Nader v. Gen. Motors Corp., 255 N.E.2d 765, 772 (N.Y. 1970) (Breitel, J., concurring))), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011) (No. 10-1259).

116. Fed. Highway Admin., *Privacy Impact Assessment: Mileage-Based Road User Charge System*, U.S. DEP'T OF TRANSP., http://www.dot.gov/pia/fhwa_nembrucs.htm (last updated May 29, 2009).

117. *Id.*; *see also A National Evaluation of a Mileage-Based Road User Charge*, UNIV. OF IOWA PUB. POLICY CTR., http://ppc.uiowa.edu/pages.php?id=65 (last visited Oct. 11, 2011) (describing generally the federal pilot program tracking vehicles with GPS technology).

will be known to others has the potential to change our behavior and ultimately who we are. These *expected* intrusions inflict upon us a different identity; they force a schism between true identity and expressed identity. In constitutional parlance, they chill the exercise of constitutionally protected activity—speech, thoughts, and behaviors—especially those that involve criticisms of the existing government or that are seen as odious by government officials.[118] The "expectation of privacy" standard has always been used to help us identify the aspects of life that are vital to our sense of well-being, aspects that have been referred to in the past as interests in privacy and now are sometimes talked about as aspects of "dignity" or interests in self-definition.[119] Expectations of privacy also play an essential role in civic and democratic life. As the Court has recognized, there is a "vital relationship between freedom to associate and privacy in one's associations. . . . Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[120] With such deep personal values at stake, the "expectation of privacy" ought to be conceived of as what the individual believes to be crucial to his or her sense of self.

One might naturally ask why a warrant requirement changes the landscape so dramatically: after all, we would still never know for sure whether we were the subject of surveillance by the government. And yet the requirement that law enforcement officials justify their surveillance decisions to judges ensures

118. *See, e.g.*, Ashcroft v. ACLU, 542 U.S. 656, 670-71 (2004) (noting that the likelihood of prosecution for speech may cause self-censorship and thus "a serious chill upon protected speech").

119. *See, e.g.*, Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."). For cases discussing privacy and dignitary interests outside the context of the Fourth Amendment, see Lawrence v. Texas, 539 U.S. 558, 574 (2003), which held that a Texas law criminalizing homosexual sodomy denies gay men and lesbians "'personal dignity and autonomy'" (quoting Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 851 (1992)); and *Casey*, 505 U.S. at 851, which described the interests recognized in cases granting constitutional protection to "personal decisions relating to marriage, procreation, contraception, family relationships, child rearing, and education" as "involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy . . . [and] central to the liberty protected by the Fourteenth Amendment." *See also* Reva B. Siegel, *Dignity and the Politics of Protection: Abortion Restrictions Under* Casey/Carhart, 117 YALE L.J. 1694, 1735 (2008) (arguing that competing conceptions of dignity in Supreme Court doctrine create a principled framework for abortion regulation).

120. NAACP v. Alabama, 357 U.S. 449, 462 (1958).

that the "machines" are watching only with good reason, not based on a whim, prejudice, or desire to discover disliked behavior. As such, it prevents the schism of self that threatens our dignitary interests.

Professor Kerr has objected that a rule requiring judges to sign off on GPS surveillance will lead to judicial confusion and inconsistency.[121] But this concern is a red herring. Simply requiring law enforcement officials to *ask* for a warrant imposes a limit on the expansion rate of the scope of surveillance. There may indeed be tough decisions for courts to make about whether limited use of GPS surveillance (e.g., tracking a suspect for a single day) triggers the Fourth Amendment warrant requirement. But this is why we have judges, and they will use all the criteria they apply to other surveillance situations—including the practical considerations about the ability to obtain a warrant—here. Even if judges grant warrants for GPS surveillance liberally, the requirement that law enforcement authorities justify each use of GPS surveillance prevents them from multiplying this monitoring by millions.

CONCLUSION

When used properly, advanced surveillance technologies significantly enhance the ability of law enforcement to maintain order and public safety. However, the Ninth Circuit's strained, mechanical application of *Knotts* and the proposed bright-line rule between behavior indoors and behavior outdoors leaves fundamental interests protected by the Fourth Amendment unguarded. Without a warrant requirement to guide its use and constrain its growth, the potential for abuse of GPS surveillance technology is vast, and its use will significantly "shrink the realm of guaranteed personal privacy."[122] Moreover, it will upset the system of checks and balances—physical as well as legal—that the Framers expected would apply to future generations. The *Jones* case affords the Supreme Court an opportunity to step in and clarify that, as with any new technologies that allow machines to do the watching, GPS surveillance technology can only be used for prolonged, automated surveillance on the authority of a warrant. Such clarification may go a long way toward resolving the confusion that the Court's prior Fourth Amendment case law has wrought.

The authors are Fellows of the Information Society Project at Yale Law School (ISP), an intellectual center addressing the implications of new information

121. *See* Kerr, *supra* note 99 ("One-month of surveillance is too long, the court says. But how about 2 weeks? 1 week? 1 day? 1 hour?").

122. Kyllo v. United States, 533 U.S. 27, 34 (2001).

technologies for law and society. Priscilla J. Smith is a Senior Fellow of the ISP, focusing on reproductive rights, privacy law, information policy, and new technologies. Smith litigated cases concerning constitutional rights to liberty, privacy, and freedom of speech for thirteen years at the Center for Reproductive Rights. She holds a J.D. from Yale Law School. Nabiha Syed is currently the First Amendment Fellow at the New York Times. *She holds a J.D. from Yale Law School and is the author of* Replicating Dreams *(2008). David Thaw is a (Postdoctoral) Research Associate in the Department of Computer Science at the University of Maryland and practices information security and privacy law in Washington, D.C. Thaw has published multiple articles and book chapters based on his research in information security, privacy, and spyware. He holds a Ph.D. (Information Management and Systems), a J.D., and an M.A. (Political Science) from the University of California, Berkeley. Albert Wong is a Ph.D. candidate in Cell Biology at Yale University. Wong has published multiple peer-reviewed articles in engineering and biology and is supported by a National Institutes of Health National Research Service Award. He holds an S.M. (Health Sciences and Technology) from the Massachusetts Institute of Technology.* *The authors would like to thank Jack Balkin, Laura DeNardis, and the other fellows of the ISP for providing us with a rich forum in which to engage on these issues and for their many important insights. They also thank the editors of* The Yale Law Journal Online *for their useful suggestions, which have greatly improved this Essay.*

Preferred citation: Priscilla J. Smith, Nabiha Syed, David Thaw & Albert Wong, *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE L.J. ONLINE 177 (2011), http://yalelawjournal.org/2011/10/11/smith.html.