

10-1259

IN THE
Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

—v.—

ANTOINE JONES,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

**BRIEF OF *AMICI CURIAE*, YALE LAW SCHOOL
INFORMATION SOCIETY PROJECT SCHOLARS AND
OTHER EXPERTS IN THE LAW OF PRIVACY AND
TECHNOLOGY IN SUPPORT OF THE RESPONDENT**

PRISCILLA J. SMITH, ESQ.

Counsel of Record

INFORMATION SOCIETY PROJECT

YALE LAW SCHOOL

319 Sterling Place

Brooklyn, New York 11238

(718) 933-9241

priscilla.smith@yale.edu

Counsel for Amici Curiae

TABLE OF CONTENTS

| | |
|--|-----|
| TABLE OF AUTHORITIES..... | iii |
| INTEREST OF <i>AMICI CURIAE</i> | 1 |
| SUMMARY OF ARGUMENT | 3 |
| ARGUMENT | 6 |
| I. The Fourth Amendment Requires a Warrant Where Invasive Surveillance Technologies Increase the Potential for Abuse. | 6 |
| II. This Court Should Continue to Prevent New Surveillance Technologies From Encroaching Protected Privacy Interests. | 10 |
| III. Prolonged GPS Surveillance Requires a Warrant Because It Invades a Reasonable Expectation of Privacy..... | 19 |
| A. Prolonged GPS Surveillance Technology is More Invasive Than Beeper Monitoring in Constitutionally Significant Ways | 20 |
| i. <i>Automated Nature of GPS</i> | 20 |
| ii. <i>Level of Detail Obtained by GPS</i> | 22 |
| iii. <i>Electronic Storage of Data</i> | 27 |

| | |
|--|----|
| B. Studies Show that People Do Not Expect to be Subjected to Pervasive Surveillance Technology Without Their Knowledge or Consent..... | 29 |
| C. GPS Surveillance Also Invades a Reasonable Expectation of Privacy Because It Is Hidden, Continuous, Indiscriminate and Intrusive..... | 34 |
| CONCLUSION..... | 36 |

TABLE OF AUTHORITIES

Cases

| | |
|---|---------------|
| <i>Ashcroft v. ACLU</i> , 542 U.S. 656 (2004) | 33 |
| <i>Byars v. United States</i> , 273 U.S. 28 (1927) | 6, 11 |
| <i>Camara v. Mun. Ct. of City & Cty. Of San Francisco</i> , 387 U.S. 523 (1967) | 6, 7 |
| <i>Dow Chemical Co. v. United States</i> , 476 U.S. 227 (1986) | 13, 18 |
| <i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001) | 23-24 |
| <i>Foltz v. Com.</i> , 698 S.E.2d 281 (Va. Ct. App. 2010) | 9 |
| <i>Illinois v. Cabelles</i> , 543 U.S. 405 (2005) | 15 |
| <i>In re Release of Historical Cell Site Information</i> , 2011 WL 3678934 (E.D.N.Y. Aug. 22, 2011) | 22, 36 |
| <i>In re Application for Historical Cell Site Data</i> , No. H-10-998M, 2010 WL 4286365 (S.D. Tex. Oct. 29, 2010) | 23 |
| <i>Katz v. United States</i> , 389 U.S. 347 (1967) | <i>passim</i> |
| <i>Kyllo v. United States</i> , 533 U.S. 27 (2001) | <i>passim</i> |
| <i>Lawrence v. Texas</i> , 539 U.S. 558 (2003) | 24 |
| <i>NAACP v. Alabama</i> , 357 U.S. 449 (1958) | 33 |

| | |
|--|---------------|
| <i>Olmstead v. United States</i> , 277 U.S. 438 (1928) | 11, 33 |
| <i>Payton v. New York</i> , 445 U.S. 573 (1980) | 7 |
| <i>People v. Weaver</i> , 909 N.E.2d 1195 (NY 2009) | 8, 9, 17, 26 |
| <i>Planned Parenthood of Se. Pa. v. Casey</i> , 505 U.S. 833 (1992) | 24 |
| <i>Schmerber v. California</i> , 384 U.S. 757 (1966) | 28 |
| <i>Stanley v. Georgia</i> , 394 U.S. 557 (1969) | 12 |
| <i>State v. Jackson</i> , 76 P.3d 217 (Wash. 2003) (<i>en banc</i>)..... | <i>passim</i> |
| <i>Treasury Employees v. von Raab</i> , 489 U.S. 656 (1989) | 25 |
| <i>United States v. Cuevas-Perez</i> , 640, F.3d 272 (7 th Cir. 2011)..... | 18, 26, 27 |
| <i>United States v. Di Re</i> , 332 U.S. 581 (1948) | 6, 25 |
| <i>United States v. Garcia</i> , 474 F.3d 994 (7 th Cir. 2007)..... | 30 |
| <i>United States v. Karo</i> , 468 U.S. 705 (1984) | <i>passim</i> |
| <i>United States v. Knotts</i> , 460 U.S. 276 (1983) | <i>passim</i> |
| <i>United States. v. Lee</i> , 274 U.S. 559 (1927) | 13, 14 |

| | |
|--|---------------|
| <i>United States v. Maynard</i> , 615 F.3d 544 (D.C. Cir. 2010)..... | <i>passim</i> |
| <i>United States v. Pineda-Moreno</i> , 617 F.3d 1120 (9 th Cir. 2010) | <i>passim</i> |
| <i>United States v. Pineda-Moreno</i> , 591 F.3d 1212 (9 th Cir. 2010), <i>Petition for Certiorari filed</i> , No. 10-1715 (docketed Nov. 17, 2010) | 16, 19 |
| <i>United States v. Torres</i> , 751 F.2d 875 (7 th Cir. 1984)..... | 34 |
| <i>United States v. U.S. District Court for the E.D. of Mich.</i> , 407 U.S. 297 (1972)..... | 7, 8, 33 |
| <i>Walter v. United States</i> , 447 U.S. 649 (1980) | <i>passim</i> |
| <i>Whalen v. Roe</i> , 429 U.S. 589 (1977) | 28 |

Miscellaneous

| | |
|---|-----------|
| 4% OF ONLINE AMERICANS USE LOCATION-BASED SERVICES (PEW RESEARCH CENTER’S INTERNET AND AMERICAN LIFE PROJECT NOV. 4, 2010), <i>available at</i> http://pewinternet.org/Reports/2010/Location- based-services.aspx | 30 |
| Susan W. Brenner, <i>The Fourth Amendment in an Era of Ubiquitous Technology</i> , 75 Miss. L. J. 1 (2005) | 6, 19, 25 |
| Suzanne Collins, <i>THE HUNGER GAMES</i> (Scholastic 2008)..... | 32 |

| | |
|--|-------|
| Thomas Y. Davies, <i>Recovering the Original Fourth Amendment</i> , 98 Mich. L. Rev. 547 (1999) | 6, 7 |
| Susan Freiwald, <i>Cell Phone Location Data and The Fourth Amendment: A Question of Law, Not Fact</i> , 70 Maryland L. Rev. 681 (2011) | 34 |
| Susan Freiwald, <i>First Principles of Communications Privacy</i> , 2007 Stan. Tech. L. Rev. 3 | 34 |
| A. Michael Froomkin, <i>The Death of Privacy?</i> , 52 Stan. L. Rev. 1461 (2000) | 35 |
| Dorothy Glancy, <i>Privacy on the Open Road</i> , 2004 Ohio Northern University Law Review 295..... | 22 |
| Eben Harrell, <i>Fighting Crime by Reading Minds</i> , TIME SCIENCE, Aug. 07, 2010, available at http://www.time.com/time/health/article/0,8599,2009131,00.html | 29 |
| Keith Hodges, <i>Tracking Bad Guys: Legal Considerations in Using GPS</i> , FEDERAL BUREAU OF INVESTIGATION LAW ENFORCEMENT BULLETIN (July 2007), available at http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/articles/FBI-LE-Bulletin-GPS-Tracking-Jul2007.pdf/view?searchterm=GPS | 9, 23 |

| | |
|---|------------|
| Ben Hubbard, <i>Police Turn to Secret Weapon: GPS Device</i> , WASHINGTON POST (Aug.13, 2008), available at http://www.washingtonpost.com/wp-dyn/content/article/2008/08/12/AR2008081203275.html . | 9 |
| Renee MacDonald Hutchins, <i>Tied Up in Knotts? GPS Technology and the Fourth Amendment</i> , 55 UCLA L. REV. 409 (2007-2008) | 18, 28 |
| Renee MacDonald Hutchins, <i>The Anatomy of a Search: Intrusiveness and the Fourth Amendment</i> , SEARCH AND SEIZURE LAW REPORT (2011) | 35 |
| Jennifer King and Chris Jay Hoofnagle, RESEARCH REPORT: A SUPERMAJORITY OF CALIFORNIANS SUPPORTS LIMITS ON LAW ENFORCEMENT ACCESS TO CELL PHONE LOCATION INFORMATION, AT 8-9 (April 18, 2008), available at http://ssrn.com/abstract=1137988 | 31 |
| <i>National Evaluation of a Mileage-based Road User Charge</i> , UNIVERSITY OF IOWA PUBLIC POLICY CENTER, available at http://www.roaduserstudy.org/Default.aspx (last visited Dec. 5, 2010) | 24 |
| <i>National Evaluation of a Mileage-based Road User Charge, Privacy of Information</i> , http://www.roaduserstudy.org/faq.aspx#privacy (last visited Dec. 5, 2010) | 24 |
| Helen Nissenbaum, <i>Privacy as Contextual Integrity</i> , 79 Wash. L. Rev. 119 (2004) | 11, 34, 35 |

| | |
|--|------------|
| PRNEWswire, <i>CAIR: FBI Sued for Warrantless GPS Surveillance of Calif. Muslim</i> , (Mar. 2, 2011), available at http://www.prnewswire.com/news-releases/cair-fbi-sued-for-warrantless-gps-surveillance-of-calif-muslim-117251848.html | 10 |
| Reva B. Siegel, <i>Dignity and the Politics of Protection: Abortion Restrictions Under Casey/Carhart</i> , 117 YALE L.J. 1694 (2008)..... | 24 |
| Christopher Slobogin, <i>Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity</i> , 72 Miss. L. Rev. 213, 235 (2002) | 29, 32, 35 |
| Daniel Solove, <i>Conceptualizing Privacy</i> , 90 Cal. L. Rev. 1087 | 34, 35, 36 |
| Peter P. Swire, <i>The System of Foreign Intelligence Surveillance Law</i> , 72 Geo. Wash. L. Rev. 1306, 1309..... | 8 |
| Kim Zetter, <i>Caught Spying on Student, FBI Demands GPS Tracker Back</i> , WIRED (Oct. 7, 2010), available at http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/all/1 | 10 |

INTEREST OF *AMICI CURIAE*¹

Amici are scholars specializing in privacy and technology law, and scholars associated with the Information Society Project at Yale Law School (ISP),² an intellectual center addressing the implications of new information technologies for law and society. They are: **Danielle Citron**, Lois K. Macht Research Professor of Law at the University of Maryland School of Law, an expert in information privacy law, former Chairperson for the AALS Section on Defamation and Privacy, and current Advisory Board Member for the SSRN *Journal on Information Privacy Law*; **Susan Freiwald**, Professor of Law at the University of San Francisco School of Law, an expert in cyberspace and information privacy law, and author of numerous articles and briefs about regulation of modern communications surveillance; **Stephen Henderson**, Professor of Law at the University of Oklahoma College of Law who writes and lectures on criminal procedure and computer crime, and serves as Reporter for the ABA Criminal Justice Standards on Law Enforcement Access to Third Party Records; **Chris Hoofnagle**, Director of the Berkeley Center for Law & Technology's information privacy programs, senior fellow to the Samuelson Law, Technology & Public Policy Clinic, and Lecturer in

¹ No counsel for a party authored this brief in whole or in part, and no person or entity other than *amici* and their counsel made any monetary contribution toward the preparation or submission of this brief. Pursuant to Supreme Court Rule 37.3, letters indicating the parties' consent to the filing of this *amicus* brief have been submitted to the Clerk.

² The Fellows participate in this case in their personal capacity; titles are used only for purposes of identification.

Residence at UC Berkeley Law School; **Renee Hutchins**, Associate Professor of Law at University of Maryland School of Law, an expert in criminal procedure, who writes on the use of GPS surveillance technology, formerly served as a federal prosecutor with the U.S. Department of Justice and a Special Assistant U.S. Attorney in the District of Columbia; **Helen Nissenbaum**, Professor of Media, Culture, Communication & Computer Science at New York University, Senior Faculty Fellow at the Information Law Institute, and author of *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE* (Stan. Univ. Press 2009); **Paul Ohm**, Associate Professor of Law at the University of Colorado Law School who writes in the areas of information privacy, computer crime, and criminal procedure; **Christopher Slobogin**, Milton R. Underwood Chair in Law, Professor of Psychiatry and Director of the Criminal Justice Program at Vanderbilt Law School, author of over 100 articles, books and chapters on criminal procedure and evidence; **Robert Ellis Smith**, publisher of *PRIVACY JOURNAL* since 1974 and author of "The Law of Privacy Explained" (2004); **Daniel Solove**, John Marshall Harlan Research Professor of Law at George Washington University Law School, an expert in privacy law and author of many books and articles on privacy, including *INFORMATION PRIVACY LAW* (Aspen, 3rd edition 2009) and *UNDERSTANDING PRIVACY* (Harv. Univ. Press 2008); and **William Staples**, Professor and Chair of Sociology at the University of Kansas, who writes on surveillance studies, privacy, law, and historical sociology.

Amici scholars associated with the ISP³ are **Jack Balkin**, Knight Professor of Constitutional Law and the First Amendment and founder and director of the ISP; **Margot Kaminski**, Research Scholar in Law and Executive Director of the ISP, who has written on law and technology issues; **Nabiha Syed**, currently First Amendment Fellow at the New York Times; **David Thaw**, Postdoctoral Research Associate in the Department of Computer Science at the University of Maryland, who has published on issues related to information security, privacy and spyware; and **Albert Wong**, ISP Fellow and Ph.D. candidate at Yale University, who has published multiple peer-reviewed articles in engineering and biology.

SUMMARY OF ARGUMENT

Advanced surveillance technologies significantly enhance law enforcement's ability to maintain order and public safety. However, in an era of rapidly advancing technologies, from thermal imagers to automated tracking devices, it is critical to ensure that these technologies are used only "in a manner which will conserve ... the interests and rights of individual citizens," *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (internal citation omitted), and conform to the Fourth Amendment. In most cases, "requiring a warrant will have the salutary effect of ensuring that use of [new technology] is not abused." See *United States v. Karo*, 468 U.S. 705, 717 (1984). The

³ Fellows of the Information Society Project at Yale Law School, Nabiha Syed, Albert Wong, and David Thaw, helped to prepare this brief under the supervision of Priscilla Smith, Senior Fellow of the ISP.

panel below correctly recognized that Global Positioning System (“GPS”) surveillance technology used for prolonged surveillance of a target’s activities in public should be subject to the warrant requirement.

The Fourth Amendment’s warrant requirement applies to a surveillance technology used in public if the technology: 1) extends beyond human capabilities for surveillance, increasing the potential for surveillance abuse; and 2) collects information the public expects to be private in a way that is not generally used and/or accepted by the general public.

In this case, first, surveillance with GPS is conducted *not by people* but by advanced tracking devices communicating with satellites in orbit and computers on the ground. As a technological substitute for traditional visual tracking, it substantially expands human capabilities far beyond “naked-eye”⁴ surveillance and vastly increases the potential for law enforcement abuse of GPS technology to conduct prolonged surveillance both against individuals as well as groups of individuals.

Second, prolonged surveillance using GPS technology intrudes on reasonable expectations of privacy under this Court’s precedents and according to tests suggested by scholarship. It provides the government with detailed information about an individual’s movements, associations, contacts and activities, allowing the storage, analysis, and comparison of that data with data gathered from others, all with minimal involvement of law

⁴ See *Kyllo*, 533 U.S. at 33.

enforcement officers. As the panel correctly held, the type and scope of information collected enables government to monitor people’s political associations, their medical treatment, and their amorous liaisons, in a way that invades their privacy and chills expression of other fundamental rights. It allows surveillance of citizens on a scale that this country has never seen and in a way that the general public has rejected.⁵

United States v. Knotts,⁶ relied on by the Government, is limited to the use of beeper technology as a sense-enhancement of, *not a replacement for*, “naked-eye” surveillance.⁷ This Court has always required warrants for the use of privacy-invading technologies that replace human or other natural senses with technological ones.⁸ Moreover, in *Knotts* this Court reserved the question of twenty-four hour dragnet surveillance using powerful new technologies.

This Court should affirm the decision of the Court of Appeals,⁹ and clarify that, while law enforcement

⁵ *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing *en banc*) (making comparison to surveillance under totalitarian regime); *United States v. Cuevas-Perez*, 640 F.3d 272, 294 (7th Cir. 2011) (Woods, J., dissenting) (GPS surveillance invites “an unprecedented level of government intrusion into every person’s private life.”).

⁶ 460 U.S. 276 (1983).

⁷ Compare *Knotts*, 460 U.S. at 282 with *Karo*, 468 U.S. at 714-15.

⁸ See *Kyllo*, 533 U.S. at 40; *Karo*, 468 U.S. at 717; *Katz v. United States*, 389 U.S. 347 (1967); *Walter v. United States*, 447 U.S. 649 (1980).

⁹ See *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

may employ GPS tracking devices in their efforts to enhance public safety, use of GPS technology in this case required a warrant to “assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.”¹⁰

ARGUMENT

I. The Fourth Amendment Requires a Warrant Where Invasive Surveillance Technologies Increase the Potential for Abuse.

The Fourth Amendment provides our primary protection against “a too permeating police surveillance” and abuse of police authority,¹¹ and “gives concrete expression to a right of the people which ‘is basic to a free society.’”¹² As has been thoroughly documented,¹³ the Framers drafted the Fourth Amendment to protect citizens against arbitrary government invasions in direct response to searches and seizures conducted under the authority of general warrants by British officers targeting

¹⁰ See *Kyllo*, 533 U.S. at 34.

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

¹² *Camara v. Mun. Ct. of City & Cty. of San Francisco*, 387 U.S. 523, 528 (1967). See also *Byars v. United States*, 273 U.S. 28, 33-34 (1927) (Fourth Amendment “adopted in view of long misuse of power in the matter of searches and seizures.”).

¹³ See, e.g., Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 *Miss. L. J.* 1, 5-7 (2005); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 *Mich. L. Rev.* 547, 741 (1999).

political opponents both in England and in the colonies.¹⁴

The Fourth Amendment's warrant requirement ensures 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."¹⁵ Without a judge's predetermination of probable cause, "the far less reliable procedure of an after-the-event justification for the . . . search [is] too likely to be subtly influenced by the familiar shortcomings of hindsight judgment."¹⁶

Moreover, the Framers designed the Fourth Amendment not only to protect personal spaces, but also to preserve an open democratic process and prevent police surveillance from being used to discourage active participation in the political process.¹⁷ As this Court recognized:

¹⁴ See, e.g., *Payton v. New York*, 445 U.S. 573, 583 & n.21 (1980); *Camara v. Mun. Ct. of City & Cty. of S.F.*, 387 U.S. 523, 528 (1967) (Fourth Amendment designed to protect "against 'arbitrary invasions.'").

¹⁵ *Id.* at 621 n.24. Indeed, historians explain that the Framers did not consider the possibility that government agents would use *their own* discretion to conduct searches, without any warrant whatsoever; they were concerned that they would overuse general warrants. See Davies, *Recovering the Original Fourth*, 98 Mich. L. Rev. at 741.

¹⁶ *Katz*, 389 U.S. at 358 (citing *Beck v. Ohio*, 379 U.S. 89, 96 (1964)).

¹⁷ See *United States v. U.S. Dist. Ct. for the E.D. Mich.*, 407 U.S. 297, 314 (1972).

History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs.¹⁸

Indeed, our freedom to discuss, disagree with, and challenge the government has depended in part on the government’s inability to continually follow all, or even large groups, of us at any time for any reason. When new surveillance technologies allow government officials to perform activities that were once prohibitively expensive or even impossible, they undermine this critical assumption and increase the possibility of abuse and its attendant danger to individual privacy. When universal surveillance becomes both feasible and cheap, officials will use it, rather than ask whether the benefits of surveillance are outweighed by the loss of constitutional values. The warrant requirement keeps constitutional protections in line with changing technology,¹⁹

¹⁸ *Id.*; see also Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L. Rev. 1306, 1309 (documenting “history of [surveillance] abuses” in the period before 1978 and that “domestic security surveillance was often executed” in ways “that posed serious threats to the democratic process.”).

¹⁹ *People v. Weaver*, 909 N.E.2d 1195 (N.Y. 2009) (noting that “without judicial oversight, the use of these powerful [GPS] devices presents a significant and, to our minds, unacceptable risk of abuse.”).

requiring government officials to justify superhuman surveillance that has become as inexpensive as flipping a switch.

Although there are no nationwide statistics available on the frequency of GPS surveillance, and most police departments resist disclosing how often they use it, evidence of widespread use exists. The FBI's training program's legal division has issued a special bulletin advising officers in the use of GPS,²⁰ and some local jurisdictions have willingly reported the scope of their use.²¹ One relatively small police department in Fairfax, Virginia, reports using GPS surveillance sixty-one times in 2005.²²

Indeed, other courts have recognized that the specter of ubiquitous surveillance is not hypothetical; it is a technological reality.²³ In one recent incident,

²⁰ See Keith Hodges, *Tracking "Bad Guys": Legal Considerations in Using GPS*, FED. BUREAU OF INVESTIGATION LAW ENFORCEMENT BULLETIN (FBI, Washington, D.C.), July 2007, at 25 ("*Tracking 'Bad Guys'*"), available at <http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/articles/FBI-LE-Bulletin-GPS-Tracking-Jul2007.pdf/view?searchterm=GPS>.

²¹ *Foltz v. Commonwealth*, 698 S.E.2d 281, 284 n.3 (Va. Ct. App. 2010) (discussing evidence of frequency of use by local law enforcement in challenge to GPS surveillance); see also Ben Hubbard, *Police Turn to Secret Weapon: GPS Device*, WASH. POST, Aug. 13, 2008, at A1 ("*Secret Weapon*").

²² Hubbard, *Secret Weapon*, *supra* n.22 at A1 (National Association of Criminal Defense Lawyers reports widespread use in large cities and small towns).

²³ See *e.g.*, *Weaver*, 909 N.E.2d at 1201 (inability to discern "any reason, apart from hunch or curiosity" for the use of GPS surveillance); *id.* at 1203 (without judicial oversight, use of GPS surveillance presents "significant and, to our minds,

a twenty-year-old American citizen and college student from Santa Clara, California, Yasir Afifi, discovered a GPS surveillance device affixed to his car. Afifi's father, also an American citizen, was president of a Muslim community association in the U.S. before moving to Egypt in 2003. Forty-eight hours after Afifi removed the device and asked for help online to identify it, he was visited by FBI agents who demanded he return the device. To date, he has not been charged with a crime, and the FBI has provided no further details.²⁴ Because the FBI obtained no warrant for the device, the public was denied the minimum level of accountability that a warrant provides.

II. This Court Should Continue to Prevent New Surveillance Technologies From Encroaching Protected Privacy Interests.

Because new technologies can create powers of surveillance that were not anticipated when old legal standards were developed, this Court evaluates the specific nature of the technology at issue and its potential for abuse.²⁵ This Court rejects "mechanical" application of standards that allow

unacceptable risk of abuse); *State v. Jackson*, 76 P.3d 217, 224 (Wash. 2003) (*en banc*) (same).

²⁴ Kim Zetter, *Caught Spying on Student, FBI Demands GPS Tracker Back*, WIRED, Oct. 7, 2010, available at <http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/all/1>. Afifi recently filed suit seeking damages. *CAIR: FBI Sued for Warrantless GPS Surveillance of Calif. Muslim*, PRNEWswire, Mar. 2, 2011, available at <http://www.prnewswire.com/news-releases/cair-fbi-sued-for-warrantless-gps-surveillance-of-calif-muslim-117251848.html>.

²⁵ Means of surveillance, not only results, determine acceptability of form of inquiry. *Kyllo*, 533 U.S. 37-39.

end-runs around Fourth Amendment protections, leaving us “at the mercy of advancing technology.”²⁶ Instead, the Court encourages adoption of rules that “take account of more sophisticated systems that are already in use or in development,”²⁷ and that will “assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted”:²⁸

[T]he assurance against any revival of [police abuse], so carefully embodied in the fundamental [Fourth Amendment] law, is not to be impaired by judicial sanction of equivocal methods, which, regarded superficially, may seem to escape the challenge of illegality but which, in reality, strike at the substance of the constitutional right.

Byars, 273 U.S. at 33-34.

This Court has modified its Fourth Amendment inquiry when necessary to ensure that the original meaning of the Amendment is carried forward. In *Katz*, the Court evaluated use of a novel listening device that attached to the *outside* of phone booths but nevertheless allowed police officers to eavesdrop on a target’s phone conversations. The officers’ actions met the technical requirements of Fourth Amendment doctrine at the time, which prohibited only *physical* intrusions into the private sphere.²⁹

²⁶ See *Kyllo*, 533 U.S. at 35-36.

²⁷ *Id.* at 37.

²⁸ *Id.* at 34.

²⁹ See *Olmstead v. United States*, 277 U.S. 438, 466 (1928). See Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash.

The Court modified the doctrine to fit new realities, recognizing that the difference between physical and electronic intrusion had “no constitutional significance.”³⁰ The Court held that the Fourth Amendment protects “people, not places,”³¹ and emphasized that notions of privacy and improper intrusion cannot be defeated by technological end-runs around previous doctrine.³²

The Court has used the distinction between sense-enhancing and sense-creating technologies to prevent surveillance from becoming ubiquitous and thus escaping the purposes of the warrant requirement. While the Court has approved the use of some primitive “sense-enhancing” technologies to aid officers conducting visual surveillance, the Court has limited their use and has *never* allowed warrantless use of sense-creating technologies—those that do not enhance human senses but substitute for human tracking.³³ For example, in *United States v. Lee*,³⁴ the Court confirmed that no search took place where officers used “searchlights”

L. Rev. 119, 132 (2004) (arguing that *Katz* reflects a change in belief about what constitutes a person’s private sphere) (“*Contextual Integrity*”).

³⁰ *Katz*, 389 U.S. at 353.

³¹ *Id.* at 351.

³² *See id.* at 362 (Harlan, J., concurring). Fourth Amendment protections go beyond the walls of each man’s “castle.” *See, e.g., Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (noting that the Framers also “protect[ed] Americans in their beliefs, their thoughts, their emotions and their sensations” (quoting *Olmstead v. United States*, 277 U.S. at 478 (Brandeis, J., dissenting))).

³³ *See Kyllo*, 533 U.S. 33; *Karo*, 468 U.S. at 717; *Walter v. United States*, 447 U.S. 649 (1980); *Katz*, 389 U.S. at 353.

³⁴ 274 U.S. 559 (1927).

or “marine glass or field glass” to help them see on the deck of a ship at night.³⁵ This limited form of sense enhancement did not implicate protections against police abuse any more than an individual officer watching without binoculars would have.

In contrast, in *Walter v. United States*,³⁶ 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. The projector did not just “enhance” sight; it created a new capacity.³⁷ The use of a technology that gave them the new ability to inspect the strip’s contents required warrant authorization.³⁸

In *Dow Chemical Co. v. United States*, the Court upheld the warrantless use of an airplane-mounted camera taking pictures of open fields below.³⁹ Nevertheless, the Court noted that sight enhancement could at some point become so significant that it created a constitutional problem, even for viewing open fields,⁴⁰ and “that surveillance of private property by using highly sophisticated

³⁵ *Id.* at 563.

³⁶ 447 U.S. 649 (1980).

³⁷ *Id.* at 652 n.2.

³⁸ *Id.* at 654. *See also Katz*, 389 U.S. at 353 (under the sense enhancement rule, no warrant would have been required if police had been able to hear a conversation through a phone booth using a simple enhancement, such as a glass placed backwards on the wall of the booth).

³⁹ 476 U.S. 227, 237-38 (1986).

⁴⁰ *See Dow Chemical v. United States*, 476 U.S. 227, 237-38 (1986) noting that the “mere fact that human vision is enhanced somewhat, *at least to the degree here*, does not give rise to constitutional problems.”).

surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.”⁴¹

United States v. Knotts, which upheld the limited use of beepers without a warrant,⁴² simply applies the sense enhancement rule of *Lee*: “[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.”⁴³ The *Knotts* Court specifically reserved the question of technology that gave the government broader surveillance powers; it declined to predict the outcome of a case in which technology allowed for “dragnet type law enforcement.”⁴⁴

United States v. Karo, decided one year later, made clear the limits 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 physically capable of

⁴¹ *Id.* at 238.

⁴² In *Knotts*, after obtaining consent from owner of a container, officers placed a beeper within a container knowing it was going to be purchased by the suspect. *Knotts*, 460 U.S. at 278. They did so only after visual surveillance made them suspicious. *Id.* Moreover, officers only used the beeper to maintain contact with the container of chloroform in the vehicle itself, not with the movements of a person. *Id.* at 282.

⁴³ *Id.* at 282.

⁴⁴ *Id.* at 283-84; see also *Maynard*, 615 F.3d at 556 (“[T]he [*Knotts*] Court specifically reserved the question whether a warrant would be required in a case involving ‘twenty-four hour surveillance.’”).

viewing.⁴⁵ Thus, as with the movie projector in *Walter*, when a beeper does not enhance human senses but replaces a human sense with a technological one, a warrant is required.⁴⁶

In *Kyllo*, this Court held that use of thermal-imaging technology to obtain “any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion” constituted a search “at least where (as here) the technology in question is not in general public use.” *Id.* at 34. While finding the thermal-imaging technology at issue there “relatively crude,” the Court in *Kyllo* advocated adopting a rule that could “take account of more sophisticated systems that are already in use or in development.” *Id.* at 36. At some point, the Court warned, technology might not just enhance human senses by allowing us to see and hear from farther distances or in the dark, but could actually create new superhuman powers, like X-ray vision, *see id.* at 36 n.3. If law enforcement had at its disposal the ability to use these non-human powers of surveillance without any warrant limitation, law enforcement technology would

⁴⁵ *Karo*, 468 U.S. at 714.

⁴⁶ The dog search cases, *see Illinois v. Caballes*, 543 U.S. 405, 408-09 (2005), holding that a sniff by a dog trained to seek illegal drugs is not a search, are different. First, because dogs are part of the natural world and were traditionally used by police to track people (and by people to hunt), the Framers would have anticipated that use. Moreover, because the sniff can only reveal evidence of illegal activity, the Court held that the only privacy interest implicated by a dog sniff is the interest in keeping illegal activity private, an interest not protected by the Fourth Amendment. *Id.*

“shrink the guaranteed realm of privacy.” *See Kylllo*, 533 U.S. at 34.

The Government suggests that the thermal imaging technology in *Kylllo* triggered the Fourth Amendment only because thermal imaging gathered information from inside a home,⁴⁷ information that the Court said would otherwise have been obtained only by “a search unequivocally within the meaning of the Fourth Amendment.”⁴⁸ However, that logic is flawed. If the officers had discovered evidence by looking into the home from outside the house using binoculars, they would have been gathering information that could otherwise only be obtained by a search of the home subject to the warrant requirement. Yet that surveillance would likely have been allowable without a warrant, because the technology (binoculars) would have been allowable sense-enhancing technology.⁴⁹

The relevant concern in *Kylllo* was not whether the information was discovered indoors or outdoors, but rather that the technology went beyond enhancement of senses, beyond binocular-like technology to the X-ray vision category. As the Court wrote, “[t]he fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth

⁴⁷ Pet. Br. at 22.

⁴⁸ *United States v. Pineda-Moreno*, 591 F.3d 1212, 1216 (9th Cir. 2010), *reh’g en banc denied*, 617 F.3d 1120 (9th Cir. 2010).

⁴⁹ The 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. *Kylllo*, 533 U.S. at 35 n.2.

Amendment.”⁵⁰ The use of a technology capable of obtaining images of heat by itself created a new sense, *substituting for* human senses, acting without human limitation or reasoning.⁵¹

Similarly, GPS surveillance does not involve “sense-enhancement,” but creates entirely new abilities beyond the capacity of even amplified human senses. As a “technological substitute for traditional visual tracking,”⁵² it should be governed by *Katz*, *Kyllo* and *Walter*, not *Knotts*. No human being can watch another’s every move twenty-four hours a day from the vantage point of outer space, remember each movement over the course of an indefinite period of time, and instantly cross-compare those movements with the pinpointed locations of other targets.⁵³ A ubiquitous vantage point, the impossibility of losing the tail, perfect memory, and the ability to instantaneously cross-reference data with police-created maps categorically differentiate GPS from the beeper used to enhance police sight-based surveillance in *Knotts*. These

⁵⁰ *Id.*

⁵¹ *Cf Knotts*, 460 U.S. 282; *id.* at 283 (noting the “limited use” which the government made of signals from beeper); *id.* at 284-85 (holding that the beeper signal was not received or relied on after it indicated that the container ended the journey during which it was tracked by a law enforcement officer); *see also United States v. Pineda-Moreno*, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) (contrasting the types of surveillance).

⁵² *See Jackson*, 76 P.3d at 223.

⁵³ *Weaver*, 909 N.E.2d at 1202-03 (relentless tracking and recording of target’s movements for 65 days “could not have been done without GPS); *Jackson*, 76 P.3d at 223 (successful uninterrupted tracking for two and one-half weeks unlikely without GPS).

abilities are not merely enhanced. They are superhuman.

In *Knotts* this Court reserved the question of prolonged, continuous surveillance presented here, as the panel recognized:⁵⁴

Knotts held only that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,” *id.* at 281, not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end.

Maynard, 615 F.3d at 557.⁵⁵ The Government tries to dismiss the Court’s concern about twenty-four hour surveillance as limited to “mass” surveillance.⁵⁶ Such a prospect is not to be taken lightly and indeed the Government’s position does not preclude such surveillance.⁵⁷ Nevertheless, the Court’s concern was

⁵⁴ *Maynard*, 615 F.3d at 556. See also *Pineda-Moreno*, 617 F.3d at 1125-26 (Kozinski, C.J., dissenting).

⁵⁵ See also *Dow Chemical*, 476 U.S. at 238 (use of satellite technology, “might be constitutionally proscribed absent a warrant.”); Renee McDonald Hutchins, *Tied up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 457 (2007) (“*Tied up in Knotts?*”).

⁵⁶ Pet. Br. at 34.

⁵⁷ See *Cuevas-Perez*, 640 F.3d at 294 (Woods, J., dissenting on other grounds) (“it is not clear why the use of GPS technology for mass surveillance would trigger the warrant requirement if the suspicionless surveillance of an individual does not.”); *Jackson*, 76 P.3d at 224 (without a warrant, there is no

broader. It included the potential for twenty-four hour surveillance of any *one* individual (“any citizen”) without judicial oversight.⁵⁸ Warrantless GPS offers the potential that *Knotts* feared.

III. Prolonged GPS Surveillance Requires a Warrant Because It Invades a Reasonable Expectation of Privacy.

As this Court recognized in *Knotts*:

this 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. [Citations omitted].

Knotts, 460 U.S. at 280-81. The Government relies on *Knotts* to argue that an individual has no reasonable expectation of privacy in his movements through public space.⁵⁹ *Knotts* held nothing of the sort.⁶⁰ Moreover, this inside/outside distinction is

limitation on GPS activity whether criminal activity is suspected or not).

⁵⁸ *Knotts*, 460 U.S. at 283 (emphasis added); see also *Pineda-Moreno*, 617 F.3d at 1126 (Kozinski, C.J., dissenting from denial of rehearing en banc) (explaining the potential for mass surveillance); *Maynard*, 615 F.3d at 556-57 (same).

⁵⁹ Pet. Br. at 17-27; see also *Pineda-Moreno*, 591 F.3d at 1216-17.

⁶⁰ See also *Pineda-Moreno*, 617 F.3d at 1125-26 (Kozinski, C.J., dissenting).

overly simplistic in the modern digital world.⁶¹ As the panel held, prolonged surveillance by invisible, automated devices that continuously gather and analyze detailed information about a person's movements for an unlimited period of time violates a reasonable expectation of privacy, constitutes a search, and requires a warrant.

A. Prolonged GPS Surveillance Technology is More Invasive Than Beeper Monitoring in Constitutionally Significant Ways.

There is a vast technical valley between the decades-old beeper technology this Court considered almost thirty years ago, and the advanced, automated GPS surveillance technology used today. Three aspects of GPS surveillance technology distinguish it from the “sense-enhancing” beeper technology considered in *Knotts* and establish its invasiveness:⁶² 1) its automated nature; 2) the level of detail obtained about a person's life; and 3) its ability to store data for long periods for analysis and comparison.

i. Automated Nature of GPS

First, the beeper in *Knotts*, was “a radio transmitter, usually battery operated, which

⁶¹ Susan Brenner, *Ubiquitous Technology*, 75 Miss. L.J. 1, 83 (2005) (“The physical and informational barriers we once used to differentiate between our ‘private’ and ‘public’ selves are being eroded by technology, and the erosion is accelerating.”).

⁶² See generally Brief of Amici Curiae Electronic Frontier Foundation (filed October 3, 2011) (“EFF Brief”) (discussing technical architecture of GPS surveillance technology).

emit[ted] periodic signals that [could] be picked up by a radio receiver.”⁶³ The signal “got stronger the closer the police were to it,” and disappeared permanently if they were too far away.⁶⁴ The beeper, considered an aid to following a vehicle through traffic, could neither determine location themselves nor store that data.⁶⁵

GPS surveillance technology, by contrast, does not merely enhance traditional police surveillance, it replaces it with something different in kind and capacity.⁶⁶ It allows remote, automated collection of data about a target’s location, movements, and speed of movement over an unlimited period of time. Once the GPS tracking device is installed, it can operate autonomously, without human involvement, independently determining and remotely transmitting positional data twenty-four hours a day. Unlike the beepers of yore, police officers need not trail the device or deploy a network of receivers in order to determine location information. As Chief Judge Kozinski puts it:

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

⁶³ *Knotts*, 460 U.S. at 277.

⁶⁴ *Pineda-Moreno*, 617 F.3d at 1124 (Kozinski, C.J., dissenting) (“If no one was close enough to pick up the signal, [the data] was lost forever.”).

⁶⁵ *Id.*

⁶⁶ *Jackson*, 76 P.3d at 223 (distinguishing GPS because officers do not actually follow vehicle).

Pineda-Moreno's case can record the car's movements without human intervention.

Pineda-Moreno, 617 F.3d at 1124 (Kozinski, C.J., dissenting).

In this way, GPS eliminates the natural limitation 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 impossible for the police to assign an officer to track large groups of citizens around the clock.⁶⁷ Now, because the GPS satellite system can support an unlimited number of tracking devices, and because GPS surveillance technology is inexpensive and allows automated tracking, neither cost nor limitations on human resources imposes an impediment to pervasive surveillance of the populace.⁶⁸

ii. Level of Detail Obtained by GPS.

Second, as the panel noted, prolonged surveillance by GPS “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.” *Maynard*, 615 F.3d at 562;

⁶⁷ Dorothy Glancy, *Privacy on the Open Road*, 2004 Ohio Northern University Law Review 295, 300.

⁶⁸ GPS surveillance technology “can provide law enforcement with a swift, efficient, silent, invisible and *cheap* way of tracking the movements of virtually anyone and everyone they choose.” *Pineda-Moreno*, 617 F.3d at 1126 (Kozinski, C.J., dissenting).

id. at 560.⁶⁹ The GPS tracking devices sense their own location and can be equipped to both store that information on the device itself and transmit that information either in real-time or in bursts to remote law enforcement computers.⁷⁰ This flexibility represents a significant advance in location tracking, allowing collection of substantially more data over prolonged periods than that gained by short bursts of beeper-based tracking.⁷¹

As the government has recognized in law enforcement training documents, this capability renders GPS tracking devices “more intrusive” than beeper-style transponders.⁷² The panel concluded that it is the *prolonged* nature of the surveillance that creates the problem, because GPS technology collects an unprecedented amount of detail on its target’s movements, and accumulation of that detail over time gives the government information about every doctor visited, political meeting attended, and

⁶⁹ See also, e.g., *In re Release of Historical Cell-Site Information*, 2011 WL 3678934 at *10-12 (E.D.N.Y. Aug. 22, 2011) (request for at least 113 days of cumulative cell-site location records for an individual’s cell phone constitutes a search under the Fourth Amendment that requires a warrant); *In re Application of the United States for Historical Cell Site Data*, No. H-10-998M, 2010 WL 4286365 at *7-8 (S.D. Tex. Oct. 29, 2010) (historical cell phone records subject to Fourth Amendment under *Maynard* because records sought “are likely far more intrusive”; they reveal “a continuous reality TV show, exposing two months’ worth of a person’s movements, activities, and associations in relentless detail.”).

⁷⁰ See generally EFF Brief.

⁷¹ *Id.*

⁷² See Hodges, *Tracking “Bad Guys,” supra* n.21, at 26.

bookstore patronized.⁷³ Prolonged GPS surveillance, as the panel concluded, invades a reasonable expectation of privacy because the detailed information obtained allows the government to develop an overall picture of people’s lives that goes far beyond what individuals expect other individuals or the government to know about their public actions.⁷⁴

This recognition by the panel that “the whole is something different than the sum of its parts,”⁷⁵ is not novel.⁷⁶ This type of analysis – rather than

⁷³ *Id.* These aspects of life—freedom of expression through speech, decisions about sexuality and medical care, belief systems, political, religious or irreligious—are vital to our dignity, our interests in self-definition. *See, e.g., Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (expectation of privacy in medical tests); *see Lawrence v. Texas*, 539 U.S. 558, 574 (2003) (interests in privacy central to personal dignity and autonomy); *Planned Parenthood of Se. Pa. v. Casey*, 505 U.S. 833, 851 (1992) (same); *see also* Reva B. Siegel, *Dignity and the Politics of Protection: Abortion Restrictions Under Casey/Carhart*, 117 YALE L.J. 1694, 1735 (2008) (competing conceptions of dignity in Supreme Court doctrine create a principled framework for abortion regulation).

⁷⁴ *Maynard*, 615 F.3d at 562 (holding “[p]rolonged surveillance reveals types of information not revealed by short-term surveillance”).

⁷⁵ *Maynard*, 615 F.3d at 561 n.8; *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”); *id.* at 561-62 (“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)).

⁷⁶ *See, e.g., Jackson*, 76 P.3d at 222 (nature and extent of information obtained concerning “a person’s associations, contacts, finances, or activities is relevant” in deciding whether expectation of privacy exists).

reliance on a line between public v. 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.”⁷⁷ The panel’s analysis has the benefit of protecting “people not places,”⁷⁸ and preventing the “too permeating police surveillance” presence warned of in *United States v. Di Re*.⁷⁹

A rule requiring judges to decide when GPS surveillance is “prolonged” would not lead to judicial confusion and inconsistency.⁸⁰ Judges have long had to evaluate complicated and often fast-paced criminal investigations to determine when a given exception applies, such as when evidence is in danger of being destroyed, a suspect is likely to flee,⁸¹ or a search serves “special governmental needs, beyond the normal need for law enforcement.”⁸² Making similar determinations about whether GPS surveillance technology is being used in a manner that should exempt it from the warrant requirement or instead in a “prolonged” manner to gather a long-term view of someone’s life is no different. For example, to the extent GPS is used to trail a fleeing suspect⁸³ an

⁷⁷ *Katz*, 389 U.S. at 351; see also Susan Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 Miss. L.J. 1, 26-27 (2005).

⁷⁸ See *Katz*, 389 U.S. at 361.

⁷⁹ *Di Re*, 332 U.S. at 595.

⁸⁰ Cf Brief of the United States at 31 (“Pet. Br.”).

⁸¹ See, e.g., *Katz*, 389 U.S. at 357-58 (discussing exceptions to rule).

⁸² See, e.g., *Treasury Employees v. Von Raab*, 489 U.S. 656, 665-66 (1989).

⁸³ Deanese Williams-Harris, *Police use GPS to track down bank robbery suspect*, CHICAGO TRIBUNE, (August 17, 2011) (police tracked bank robber’s movements through a GPS device hidden

exception to the warrant requirement would apply. In fact, the rule is already being applied in the states which have held that warrants are required for GPS surveillance under state constitutions.⁸⁴

Moreover, the *Maynard* panel did not consider use of GPS to follow a suspect on a single trip “prolonged” use requiring a warrant.⁸⁵ For example, in *United States v. Cuevas-Perez*,⁸⁶ the court distinguished the use of GPS surveillance of a single trip over sixty hours from the twenty-eight day surveillance in *Maynard*. In that case, “[u]nlike in *Maynard*, the surveillance . . . was not lengthy and did not expose, or risk exposing, the twists and turns of Cuevas-Perez’s life, including possible criminal activities, for a long period.”⁸⁷ In contrast, GPS monitoring performed by machines and designed to gather data to expose patterns of behavior, such as that in *Pineda-Moreno* and *Maynard*, should be considered prolonged and require a warrant. There

with cash he stole), <http://www.chicagotribune.com/news/local/breaking/chi-police-use-gps-to-track-down-bank-robbery-suspect-20110817,0,3267869.story>.

⁸⁴ Washington, New York, Oregon, and Massachusetts require a warrant for police surveillance via GPS devices. *Weaver*, 909 N.E.2d at 1201-03; *Commonwealth v. Connolly*, 913 N.E.2d 356 (Mass. 2009); *Jackson*, 76 P.3d at 222-24; *State v. Campbell*, 759 P.2d 1040 (Or. 1988).

⁸⁵ *Maynard*, 615 F.3d. at 565 (“[s]urveillance that reveals only what is already exposed to the public—such as a person’s movements during a single journey—is not a search.”) (citing *Knotts*, 460 U.S. at 285).

⁸⁶ 640 F.3d 272 (7th Cir. 2011).

⁸⁷ *Id.* at 274-75; *but see id.* at 292-93 (Woods, J., dissenting) (stating “the majority’s assertion that Cuevas–Perez’s movements in this case can be categorized as a “single journey” under *Maynard’s* reasoning, . . . is simply untenable”).

may indeed be tough decisions for courts to make about whether an uninterrupted single trip constitutes prolonged use but first of all, that is not the situation in this case. Moreover, where it is the case, judges may consider the same criteria applied to other surveillance situations, such as the practical ability to obtain a warrant, in making those calls.

iii. Electronic Storage of Data.

Third, the electronic storage of gathered location data allows the data to be stored forever and considered alongside data collected from other sources. In contrast to beeper data which is lost because an individual does not record and store it, GPS computers can be programmed to operate independently and compare data gathered from different individuals, identifying common patterns of behavior and the gatherings of different groups of people.⁸⁸ 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?

⁸⁸ Cf. *Pineda-Moreno*, 617 F.3d at 1124 (Kozinski, C.J., dissenting from denial of rehearing en banc) (distinguishing GPS system from beeper system on the basis that without human involvement, beeper data was “lost forever”).

Pineda-Moreno, 617 F.3d at 1125 (Kozinski, C.J., dissenting). The new GPS technology is capable of retaining information forever, making those who have been tracked vulnerable to intrusive data analysis of where they went, and who they saw, for years after the fact.

Taken seriously the Court's mandate that we must not allow new technology to "shrink the private realm" requires us to examine the impact that the new means of surveillance will have on our privacy expectations.⁸⁹ We can not afford to revive the rejected doctrine of a strict line between public and private space dependent on notions of physical trespass.⁹⁰ As technology does things the Framers never thought possible, it changes what it means to cross into the private realm. If we eventually develop a means of reading minds,⁹¹ it won't matter if that technological invasion takes place in the home or on the streets.

⁸⁹ *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.").

⁹⁰ See also Hutchins, *Tied up in Knotts?*, *supra* n. 63, at 432 (arguing that warrant rule must apply because technology develops broad view of individuals).

⁹¹ See Eben Harrell, *Fighting Crime by Reading Minds*, TIME SCIENCE, Aug. 07, 2010, available at <http://www.time.com/time/health/article/0,8599,2009131,00.html>.

B. Studies Show that People Do Not Expect to be Subjected to Pervasive Surveillance Technology Without Their Knowledge or Consent.

Further supporting reasonable expectations of privacy in our movements, and as the panel correctly noted, we have not become a society that expects constant surveillance of our daily activities.⁹² As Chief Judge Kozinski recognized,

You 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.

617 F.3d at 1126 (Kozinski, C.J., dissenting). We value the privacy of data revealing our location and we actively resist relinquishing our ability to remain anonymous in public. Many Americans are comfortable with use of a GPS service to determine their own personal location when that service operates subject to their consent and control.⁹³ The

⁹² *Maynard*, 615 F.3d at 563 (“A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car”; “rather, he expects each of those movements to remain ‘disconnected and anonymous.’”). *See also* *Kyllo v. United States*, 533 U.S. 27, 28 (2001) (examining whether technology was in general public use); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 *Miss. L. Rev.* 213, 235 (2002) (“Camera Surveillance”) (arguing that the Fourth Amendment protects a right to anonymity).

⁹³ Subscription services such as LoJack and OnStar can access an automobile’s location and even transmit this location in case of emergency or theft, but only do so with the consent of the

public does not, however, accept unrestrained GPS *surveillance* technology; we retain an expectation that we are not being followed perpetually by an invisible computerized eye in the sky. In fact, Americans become uncomfortable with GPS when it leads to even a slight loss of user-control and threatens the loss of public anonymity.

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 their phones, only four percent of adult Americans use these services.⁹⁴ Moreover, a 2008 survey conducted by the Samuelson Law, Technology & Public Policy Clinic at UC Berkeley School of Law found that 73% of survey participants supported strong judicial intervention before law enforcement could access historical location data.⁹⁵

user. Contrary to Judge Posner’s assertion, Google Earth, the web service providing satellite images of the ground, cannot track people or vehicles in real time. *See United States v. Garcia*, 474 F.3d 994, 997 (7th Cir. 2007).

⁹⁴ 4% OF ONLINE AMERICANS USE LOCATION-BASED SERVICES at 2 (PEW RESEARCH CENTER’S INTERNET AND AMERICAN LIFE PROJECT NOV. 4, 2010), *available at* <http://pewinternet.org/Reports/2010/Location-based-services.aspx>.

⁹⁵ Jennifer King and Chris Jay Hoofnagle, RESEARCH REPORT: A SUPERMAJORITY OF CALIFORNIANS SUPPORTS LIMITS ON LAW ENFORCEMENT ACCESS TO CELL PHONE LOCATION INFORMATION, AT 8-9 (April 18, 2008), *available at* . It follows from this desire to protect anonymity in public, that people would view surreptitious attachment of GPS surveillance devices on their cars as a “meaningful interference with an individual’s possessory interest in that property.” *See Karo*, 468 U.S. at 712

In another context, the federal government has recognized that members of the American public maintain a reasonable expectation of privacy in 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.”⁹⁶ Organizers also assured participants that they would maintain information about mileage in “highly secure locations” in a separate database on a separate server from their personal information.⁹⁷ The organizers’ assurances indicate their recognition of a reasonable expectation of privacy in data about public movements.

Some commentators have criticized taking the public’s reaction to surveillance technology into account, pointing out that the expectation of privacy does not hinge on whether monitoring is likely to occur or whether the public expects monitoring to

(quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). See also Brief for Respondent at 50-52.

⁹⁶ *National Evaluation of a Mileage-based Road User Charge, Privacy of Information*, UNIVERSITY OF IOWA PUBLIC POLICY CENTER, available at <http://www.roaduserstudy.org/faq.aspx#privacy> (last visited Dec. 5, 2010).

⁹⁷ *National Evaluation of a Mileage-based Road User Charge*, UNIVERSITY OF IOWA PUBLIC POLICY CENTER, <http://www.roaduserstudy.org/Default.aspx> (last visited Dec. 5, 2010) (describing federal pilot program tracking vehicles with GPS); See *id.* & video available at <http://www.roaduserstudy.org/howitworks.aspx>. (last visited Dec. 3, 2010).

occur. However, taking into account the public's *resistance* to technology that will track their every movements is relevant to a showing of the private nature of location data. Of course, as in Orwell's *1984*,⁹⁸ and the contemporary children's book *The Hunger Games*,⁹⁹ when the occurrence and expectation of monitoring both increase and thus the expectation of freedom from monitoring diminishes, constitutionally protected privacy interests suffer greatly.¹⁰⁰ As many have noted, when our activities, thoughts, and behaviors become known to others, our sense of self shrinks—from shame, from fear, from embarrassment, or simply from a loss of the ability to control the distribution of information about us.¹⁰¹ The expectation that these “private” matters will become known will change our behavior and ultimately who we are. In constitutional parlance, it chills the exercise of constitutionally protected activity, speech, thoughts, and behaviors—especially those that involve criticisms of the existing government or that are seen as undesirable by

⁹⁸ While the world of Orwell's *1984* may be our most culturally recognizable icon of totalitarianism and as such is an overused reference point, it is no less illustrative for that status.

⁹⁹ Suzanne Collins, *THE HUNGER GAMES* (Scholastic 2008) (describing society where the activities of citizens are monitored and, in some instances, broadcast over television).

¹⁰⁰ See, e.g., *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) (discussing surveillance under a totalitarian regime).

¹⁰¹ Christopher Slobogin, *Camera Surveillance*, 72 *Miss. L. Rev.* at 236 (anonymity in public promotes “open society”; “Lack of public anonymity promotes...an oppressive society.”).

government officials.¹⁰² Indeed, if individuals have come to expect that information about their every movement *is* being collected and stored for analysis, then a fundamental goal of the Framers has been abandoned. Maintaining privacy in group associations “may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.”¹⁰³

While we presume that most law enforcement officers use tracking devices in good faith, this Court has recognized that the warrant requirement provides a crucial check on misuse of these powerful tactics.¹⁰⁴ Used *with* a warrant requirement, GPS surveillance technology gives law enforcement a powerful crime fighting tool that will not invade privacy unnecessarily. *See Karo*, 468 U.S. at 717 (warrants prevent abuse of technology). *Without* a warrant requirement, GPS, like wiretaps and thermal imaging devices, “shrink[s] the realm of personal privacy,” *Kyllo*, 533 U.S. at 34, beyond the dreams or nightmares of the Framers.

¹⁰² *See, e.g., Ashcroft v. ACLU*, 542 U.S. 656, 670-71 (2004) (likelihood of prosecution for speech may cause “serious chill upon protected speech”).

¹⁰³ *NAACP v. Alabama*, 357 U.S. 449, 462. “[W]rits of assistance and general warrants are but puny instruments of tyranny and oppression” when compared with the power of GPS surveillance technology. *See Olmstead*, 277 U.S. at 476 (Brandeis J., dissenting).

¹⁰⁴ *See, e.g., U.S. Dist. Ct.*, 407 U.S. at 314.

C. GPS Surveillance Also Invades a Reasonable Expectation of Privacy Because It is Hidden, Continuous, Indiscriminate and Intrusive.

GPS surveillance also invades a reasonable expectation of privacy using a four factor test proposed for determining whether there is an expectation of privacy in location data.¹⁰⁵ Borrowing from a decision by Judge Posner concerning the nature of television surveillance,¹⁰⁶ Susan Freiwald argues that surveillance that reveals location information should be judged by whether it is hidden, continuous, indiscriminate and intrusive.¹⁰⁷ Others scholars, pointing out that *where* behavior occurs is not always determinative of the private nature of that behavior,¹⁰⁸ have proposed similar tests for evaluating the intrusiveness of a surveillance technology,¹⁰⁹ and for evaluating the

¹⁰⁵ Susan Freiwald, *Cell Phone Location Data and The Fourth Amendment: A Question of Law, Not Fact*, 70 Maryland L. Rev. 681, 746 (2011) (“*Cell Phone Location Data*”); Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech. L. Rev. 3.

¹⁰⁶ See *United States v. Torres*, 751 F.2d 875, 882-85 (7th Cir. 1984) (television surveillance is exceedingly intrusive and could be abused to eliminate privacy).

¹⁰⁷ *Cell Phone Location Data*, 70 Maryland L. Rev. at 746.

¹⁰⁸ Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. at 1144-45 (“privacy must be valued contextually.”); Nissenbaum, *Contextual Integrity*, 79 Wash. L. Rev. at 138.

¹⁰⁹ See Renee MacDonald Hutchins, *The Anatomy of a Search: Intrusiveness and the Fourth Amendment*, SEARCH AND SEIZURE LAW REPORT (2011) (advocating adoption of intrusiveness as the benchmark for assessing a search and requiring an examination of two factors: the functionality of a challenged

specific context in which the surveillance technology is being used to determine whether a violation of privacy has occurred.¹¹⁰ As Helen Nissenbaum argues, “the 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 . . . ‘none of your business,’ to a stranger asking their names.”¹¹¹ Similarly, A. Michael Froomkin writes 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.”¹¹² In fact, in light of the impossibility of keeping all information secret in the digital age, clinging to the idea of privacy as a form of total secrecy “would mean the practical extinction of

form of surveillance and the potential for disclosure created by the device); Christopher Slobogin, *Camera Surveillance*, 72 Miss. L. Rev. at 270 (examining privacy expectations through study of subjects’ sense of the intrusiveness of public surveillance using video cameras).

¹¹⁰ Nissenbaum, proposes that whether 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 . . . ; and the terms of further dissemination.” Nissenbaum, *Contextual Integrity*, 79 Wash. L. Rev. at 155.

¹¹¹ Nissenbaum, *Contextual Integrity*, 79 Wash. L. Rev. at 139; *id.* at 143 (arguing that “a privacy violation has occurred when . . . contextual norms of appropriateness . . . have been breached.”).

¹¹² A. Michael Froomkin, *The Death of Privacy?*, 52 Stan. L. Rev. 1461, 1476 (2000).

privacy in today's world."¹¹³ Under all of these tests, GPS surveillance requires a warrant.¹¹⁴

CONCLUSION

The panel's approach to evaluating privacy expectations in public behavior will preserve privacy in a digital age and protect the public from overuse of law enforcement surveillance. Without a warrant requirement to guide its use, the potential for abuse of GPS surveillance technology is unprecedented and its use will significantly "shrink the realm of personal privacy." *See Kyllo*, 533 U.S. at 34. Therefore, the court should affirm the decision below.

Respectfully submitted,

PRISCILLA J. SMITH, ESQ.

(Counsel of Record)

INFORMATION SOCIETY PROJECT

YALE LAW SCHOOL

319 STERLING PLACE

BROOKLYN, NY 11238

Counsel for Amici Curiae

October 3, 2011

¹¹³ Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. at 1155.

¹¹⁴ *See In re Release of Historical Cell-Site Information*, 2011 WL 3678934 at *10-12.