	SUPREME COURT OF NEW JERSEY DOCKET NO. 68,765 Appeal No. A-53-11
STATE OF NEW JERSEY, Plaintiff	Criminal Action
v.	On Appeal from a Final Order of the Superior Court, Appellate Division, Affirming the Judgment of Conviction
Thomas W. Earls, Defendant	Sat Below: Hon. Anthony J. Parrillo, JAD Hon. Patricia B. Roe, JAD Hon. Stephen Skillman, JAD

BRIEF OF *AMICUS CURIAE*
ELECTRONIC PRIVACY INFORMATION CENTER

On the brief:
Grayson Barber
Marc Rotenberg
Alan Butler
David Jacobs

GRAYSON BARBER
Grayson Barber, LLC
68 Locust Lane
Princeton, NJ 08540
(609) 921-0391
Counsel of Record for Proposed Amicus Curiae Electronic Privacy Information Center

MARC ROTENBERG
Electronic Privacy Information Center
1718 Connecticut Ave NW
Suite 200
Washington, DC 20009
(202) 483-1140

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

REGULATIONS

INTEREST OF AMICUS

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.[1]

EPIC has participated as amicus curiae before this Court, *G.D. v. Kenny*, 205 N.J. 275 (2011); *State v. Reid*, 194 *N.J.* 386 (2008), and in many other jurisdictions, concerning privacy issues, new technologies, and constitutional interests. *See, e.g., US v. Jones*, 132 S. Ct. 945 (2012); *Doe v. Reed*, 529 F.3d 892 (9th Cir. 2008), *cert. granted,* 130 S. Ct. 1011 (U.S. Dec. 14, 2009) (No. 09-559); *Flores-Figueroa v. United States*, 129 S. Ct. 1886 (2009); *Herring v. United States*, 129 S. Ct. 695 (2009); *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Department of Justice v. City of Chicago*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002); Reno v. Condon, 528 U.S. 141 (2000); *National Cable and*

[1] This brief was prepared with the assistance of Maria Elena Stiteler, a law student at Stanford Law School and participant in the EPIC Internet Public Interest Opportunities Program (IPIOP).

Telecommunications Association v. Federal Communications Commission, 555 F.3d 996 (D.C. Cir. 2009); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006) 470 F.3d 1104 (5th Cir. 2006); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); and *State v. Raines*, 857 A.2d 19 (Md. 2003).

EPIC has a particular interest in the impact of new surveillance technologies that have the capacity to enable warrantless, pervasive mass surveillance of the public by law enforcement agents. EPIC filed briefs on this issue in US v. Jones, 132 S. Ct. 945 (2012) and Commonwealth v. Connolly, 454 Mass. 808 (2009). Such techniques offend the right of individuals to maintain their privacy and their right to be free of unreasonable searches. EPIC has routinely urged courts to take meaningful steps towards protecting the privacy of individuals as they travel through public and private spaces.

SUMMARY OF THE ARGUMENT

This case presents the question of whether an individual has a reasonable expectation of privacy in the current location of their cell phone. The Supreme Court recently held that the use of a GPS tracking device installed on a car was a Fourth Amendment search because the government "physically occupied private property for the purpose of obtaining information." *United States v. Jones*, 132 S. Ct. 945, 949 (2012). A majority of the Justices, writing in two separate concurrences, further indicated that the use of a GPS tracking device also violated the reasonable expectation of privacy test set out in *United States v. Katz*, 389 U.S. 347 (1967). The location tracking methods at issue in this case are far more invasive than those in *Jones*, involving the collection of more personal data that can be compiled over a long period of time, which is both more detailed and more revealing. Moreover, cell phone tracking occurs on an enormous scale throughout the United States. In light of the Supreme Court's decision in *Jones*, this court should hold that an individual has a reasonable expectation of privacy in the location of their cell phone. Without robust Fourth Amendment protections, the use of location tracking techniques will allow suspicionless tracking, monitoring, and profiling of Americans without judicial review.

ARGUMENT

This case presents the question of whether an individual has a reasonable expectation of privacy in the current location of his cell phone. *State v. Earls*, 420 N.J. Super. 583, 591 (App. Div. 2011). The Supreme Court in *United States v. Jones* ruled that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" 132 S. Ct. 945, 949 (2012). Five of the Justices signed two concurring opinions that stressed the importance of location privacy and strongly suggested that the use of GPS location tracking devices would also have violated the Fourth Amendment under the *Katz* reasonable expectation of privacy test. *See id.* at 954-57 (Sotomayor, J., concurring) and 957-64 (Alito, J., concurring). In this case, the method used (real-time cell phone tracking) is uniquely invasive and threatens to chill constitutionally protected activities. Cell phone location tracking is especially invasive in urban areas where it can be even more accurate than the GPS tracking at issue in *Jones*. Individuals have clearly expressed their legitimate and reasonable expectation that location information generated by their cell phones and other devices is private.

I. Real-Time Cell Phone Location Tracking Is More Invasive than the GPS Tracking in *Jones*; Judicial Oversight Is Necessary to Prevent Abuse

In *Jones*, Justice Sotomayor agreed with Justice Scalia that the case before the Court could be resolved because the violation arose from the simple trespass and subsequent monitoring of an individual operating a vehicle. She wrote separately to emphasize that location tracking methods which "generat[e] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations" would violate an individual's reasonable expectation of privacy. *Id.* at 955 (Sotomayor, J., concurring). Justice Sotomayor warned, "[a]wareness that the Government may be watching chills associational and expressive freedoms." *Id.* at 956. These threats to constitutionally protected interests are more severe with cell phone location than with the location of an automobile at issue in *Jones*. For most Americans, a cell phone is an ever-present accessory, necessary for work, school, and everyday social and political life and kept on their person at all times.

A. The Accuracy of Network-Based Location Tracking Methods Is as Good as or Greater than GPS in Most Cities, and It Is Increasing as Technology Evolves

Current technology allows cell phone service providers to pinpoint the location of an individual's cell phone with increasing accuracy. CTIA: The Wireless Ass'n, *Wireless in*

America: FAQ (May 2011).[2] Currently, the Federal Communications Commission requires cellular carriers to identify the location of cell phone users when dialing 911 to within "100 meters for 67 percent of calls." FCC Regulations on Enhanced 911 Emergency Services, 47 C.F.R. § 20.18 (2011). Service providers can achieve even more accurate location information with advanced network-based location tracking techniques. *See* ABI Research, *TruePosition Whitepaper* (July 14, 2011).[3] Each cell phone accesses its service provider network through a series of radio base stations ("cell sites"), and periodically identifies itself with nearby cell sites (a process called "registration"). *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 111th Cong. 20 (2010) (testimony of Matt Blaze, Professor, University of Pennsylvania) [hereinafter *Professor Matt Blaze*]. Based on the data gathered by these cell sites, a service provider can use network-based location methods ("triangulation") to determine the location of a cell phone. Gina Stevens et al., Cong. Research Serv., *Legal Standard for Disclosure of Cell. Research Service-Site Information (CSI) and Geolocation Information* (June 29, 2010).[4] The practical accuracy

[2] *Available at* http://files.ctia.org/pdf/WirelessInAmerica_Jan2011.pdf.
[3] *Available at* http://www.trueposition.com/white-papers/.
[4] *Available at* http://www.fas.org/sgp/crs/intel/crs-csi.pdf.

of network-based location tracking methods depends on various factors, including the number of cell sites in the area. Jeffrey E. Bull, *Wireless Geolocation: Advantages and Disadvantages of the Two Basic Approaches for E-911*, IEEE Vehicular Technology Magazine Dec. 2009, at 45, 50. The typical cell sector size has been shrinking as the user base and density has increased. CTIA: The Wireless Ass'n, *Wireless in America: How Wireless Works* (May 2011). The radio base stations can be as small as "a conventional stereo speaker." *In re US for Historical Cell Site Data*, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010). Industry estimates show that the total number of cell sites in the United States has increased from 913 to more than 251,000 since 1986. *Id.* at 832; *U.S. Wireless Quick Facts*, CTIA: The Wireless Ass'n.[5]

As cell site density increases, and technology improves, the precision of network-based location tracking will continue to increase. Already, the high density of microcells in urban areas means that the location range "can be small enough to identify individual floors and rooms within buildings." *Professor Matt Blaze* at 25. Even the lower court in this case acknowledged that the "cell-site data is simply a proxy" for

[5] The current number of cell sites as of June 2011 is 256,920. *U.S. Wireless Quick Facts*, CTIA: The Wireless Ass'n, http://www.ctia.org/media/industry info/index.cfm/AID/10323 (last visited Feb. 28, 2012).

user location. *State v. Earls*, 420 N.J. Super. 583, 597 (App. Div. 2011).

A recent report from ABI Research, a market intelligence company specializing in "global connectivity and emerging technology," About ABI Research, ABI Research, [6] shows that current network-based location tracking methods [7] are more accurate in urban and suburban environments than GPS tracking methods. [8] *TruePosition Whitepaper*, ABI Research, July 14, 2011. These network-based methods are effective regardless of the particular cell phone used, and allow accurate location tracking of a device indoors. *Id.* at 5. The tests conducted by ABI Research showed that the network-based methods used by TruePosition were effective to within a 78-meter radius indoors, versus a 160-meter radius for the most effective GPS methods. *Id.* at 9. [9] It is already clear that GPS tracking methods are invasive. *See generally Jones*, 132 S.Ct. 954. Current network-based methods are *more* effective indoors than GPS makes them

---

[6] http://www.abiresearch.com/about.jsp.

[7] Specifically Uplink Time Difference of Arrival (U-TDOA) which is used by TruePosition. *See* ABI Research, *TruePosition Whitepaper* (July 14, 2011) *available at* http://www.trueposition.com/white-papers/.

[8] Specifically Assisted GPS (A-GPS) used by many wireless carriers. *Id.*

[9] The test included more than 3,500 real wireless 911 calls, and showed that U-TDOA performed well in both indoor and outdoor locations (78.3m – 168.6m for 67th-95th percentiles outoors and 77.5m – 239.4m for 67th-95th percentiles indoors) while A-GPS performed very poorly in indoor locations (157.6m – 1088.2m for 67th-95th percentiles outdoors). *Id.* at 9.

more invasive because it allows the government to identify particular buildings, offices, and businesses that an individual visits.

B. The Vast Majority of Americans Own Cell Phones, And Law Enforcement Location-Information Requests Occur at an Astonishing Rate

Currently, eighty-three percent of Americans own cell phones, Aaron Smith, Pew Research Center, *Americans and Their Cell Phones* (Aug. 15, 2011),[10] and a growing portion of these users own smart phones, which enable location-based services and location-based tracking. *See* Nielson Research, *More US Consumers Choosing Smartphones as Apple Closes the Gap on Android* (Dec. 15, 2011).[11] Individuals increasingly rely on cell phones as their primary means of communication, and they carry the phones wherever they go. Cell phones are essential to the everyday lives of students, Marc Prensky, *What Can You Learn from a Cell Phone? Almost Anything!*, 1 Innovate! 5 (2005),[12] and workers. *See* Verne G. Kopytoff, *More Offices Let Workers Choose Their Own*

[10] *Available at* http://www.pewinternet.org/~/media//Files/Reports/2011/Cell%20Phones%202011.pdf.

[11] *Available at* http://blog.nielsen.com/nielsenwire/consumer/more-us-consumers-choosing-smartphones-as-apple-closes-the-gap-on-android/ (stating that 46% of mobile users own smart phones, and 60% of new mobile phone purchases were smart phones)

[12] *Available at* http://innovateonline.info/pdf/vol1_issue5/What_Can_You_Learn_from_a_Cell_Phone__Almost_Anything!.pdf.

Devices, NYTimes, Sept. 22, 2011.[13] The total penetration of wireless devices in the United States rose above 100% in 2011. *U.S. Wireless Quick Facts*, CTIA: The Wireless Ass'n.[14] This means that there are more cell phones than people in the United States. As of June 2010, more than one in four US households had only wireless telephones. *See* Stephen J. Blumberg, Ph.D., et al., *Wireless Substitution: State-level Estimates from the National Health Interview Survey, January 2007-June 2010*, 39 Nat'l Health Stat. Rep. 1 (2011).[15]

Without strong Fourth Amendment protections for important and personal location data, law enforcement will continue to track individuals with increasing frequency. Already, law enforcement agencies request subscriber information from service providers like Verizon at an astonishing rate. *See* Christopher Soghoian, *The Law Enforcement Surveillance Reporting Gap* 3 n.6 (April 10, 2011) (unpublished manuscript) ("According to a letter sent by a Verizon executive to members of Congress in

---

[13] *Available at* http://www.nytimes.com/2011/09/23/technology/workers-own-cellphones-and-ipads-find-a-role-at-the-office.html?pagewanted=all.

[14] *Available at* http://www.ctia.org/media/industry info/index.cfm/AID/10323 (last visited Feb. 24, 2012).

[15] *Available at* http://www.cdc.gov/nchs/data/nhsr/nhsr039.pdf.

2007, the company receives approximately 90,000 requests from law enforcement agencies each year.").[16]

In fact, such requests are so frequent that some service providers have begun automating the process by "developing a web interface that gives agents direct access to users' location data." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, J. dissenting to denial of rehearing en banc). These service provider "back doors" are particularly susceptible to abuse. A single service provider, Sprint Nextel, provided law enforcement with customer location information over eight million times between September 2008 and October 2009. *See* Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times Over A* Year, Wired, Dec. 1, 2009.[17]

[16] *Available at* http://ssrn.com/abstract=1806628.
[17] *Available at* http://www.wired.com/threatlevel/2009/12/gps-data/.

C. Location Data Reveals a Great Deal About an Individual, and Location Tracking Tools Can Be Abused and Create Chilling Effects

When a government agency gathers cell phone location data, they are compiling a great deal of information about the individual cell phone user. "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010) *aff'd in part sub nom. United States v. Jones*, 132 S. Ct. 945 (U.S. 2012). Even real-time tracking data will naturally be compiled and analyzed over a period of hours, days, weeks, or months to identify patterns and discern relevant information.[18]

In urban areas where cell sites are tightly packed to accommodate increased population density, network-based location tracking can potentially distinguish between floors or even rooms within a building, and today, technological advances allow the government to use the mobile network to track the location

[18] Consider, for example, the facts of this case, where the New Jersey officers requested the Defendant's location information three separate times before locating his car. They no doubt recorded the results of each request, and thus discerned information about whether he was stationary or moving during that three-hour period, as well as his general location.

of cellular phone calls within fifty yards. *See supra* Part I.A. This level of accuracy allows police to obtain a "precise, comprehensive record" of a cell phone user's "familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 956 (2012) (Sotomayor, J., concurring).

Location tracking techniques allow for extraordinary intelligence gathering, but they also enable abuse. There have already been reported examples of abuse of these tools. For example, police officers in Michigan requested information due to a "riot" in an area "where a labor-union protest was expected," and a police officer improperly demanded the location of his daughter based on a claim that she was "kidnapped" (she was actually out with friends). *See* Michael Isikoff, *The Snitch in Your Pocket*, Newsweek, Mar. 1, 2010.[19]

State and federal agencies plan to increase the scope and pervasiveness of location tracking techniques by contracting with private firms. Already private companies such as TruePosition provide location intelligence ("LOCINT") services to cell phone service providers, and thus to law enforcement officials who rely on those providers. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 111th Cong. 20 (2010) (testimony of Michael Amarosa,

[19] *Available at* http://www.newsweek.com/id/233916.

Senior Vice President for Public Affairs, TruePosition). *See* Jeffrey E. Bull, *Advantages and Disadvantages of the Two Basic Approaches for E-911*, IEEE Vehicular Tech. Mag. Dec. 2009 at 45, 50.[20] This LOCINT technology provides the government with the "ability to use data and information about spatiotemporal relationships between and among people, places, and objects to understand actions and events that have occurred or are occurring." *See* Mark Kagan, TruePosition, *Location Intelligence and Surveillance for the Security and Law Enforcement Toolkit*, White Paper, TruePosition, Oct. 2008 at 7 (hereinafter *TruePosition Law Enforcement Toolkit*).

The Government has promoted the development of advanced location tracking methods for use in locating the origin of 911 calls made from cell phones. But these tracking methods also dramatically expanded the scope of information available to law enforcement. Richard Barnes, et al., *Internet Geolocation and Location-Based Services*, IEEE Comm. Mag., Apr. 2011 at 102. In particular, companies like TruePosition provide the capacity to "locate all mobile phones with very high accuracy ... in any environment," and to "analyze forensic location intelligence data." *TruePosition Law Enforcement Toolkit* at 9. This service would gives law enforcement the ability to "detect suspicious

[20] Jeffrey Bull is the senior director of technology at TruePosition, Inc. *Id.*

behavioral patterns," "reveal the physical identity of subjects," and "mine historical mobile phone data to detect relationships." *Id.* at 10. The capacity to reveal an individual's *associations* and *expressions* is not only a side effect of these location tracking methods, it is the intended result. The tools available to government officials enable the type of intrusive surveillance that "chills associational and expressive freedoms" as Justice Sotomayor noted recently in *United States v. Jones*, 132 S. Ct. at 956 (J. Sotomayor, concurring). These location tracking methods must be subject to traditional Fourth Amendment protections in order to ensure that the process is not abused.

II. Cell Phone Location Tracking Involves "a Degree of Intrusion That a Reasonable Person Would Not Have Anticipated" According to the Alito Concurrence in *United States v. Jones*

A. Cell Phone Location Tracking Involves Privacy Violations that Reasonable Users Do Not Anticipate

Consumers generate enormous amounts of location information while using their phones, although use of this information often occurs without their knowledge or consent. A recent survey found that seventy-seven percent of cell phone users did not want to disclose their location to application owners or developers. Harris Interactive, *Mobile Privacy: A User's Perspective* (Mar.

4, 2011).[21] Other surveys found that although users are aware that cell phones disclose location data, they are concerned about controlling who has access to their location. Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls* (2010).[22]

Cell phone users do not expect that their devices will be secretly used to track their location and object when such practices are revealed. Indeed, consumers strongly object when companies secretly enable location tracking services. *See* John R. Quain, *Changes to OnStar's Privacy Terms Rile Some Users*, N.Y. Times, Sept. 22, 2011.[23] In May 2011, data scientists revealed that an unencrypted file on Apple iPhones stored a ten-month record of a user's location data. *See* Nick Bilton, Tracking File Found in iPhones, N.Y. Times, Apr. 20, 2011.[24] In response, members of Congress and the media criticized Apple. *See* Letter from Al Franken, Chairman, Subcommittee on Privacy, Technology and the Law, to Steve Jobs, CEO, Apple Corp. (Apr.

---

[21] *Available at* http://www.scribd.com/doc/54220855/TRUSTe-Mobile-Privacy-Report.
[22] *Available at* http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.
[23] *Available at* http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users.
[24] *Available at* https://www.nytimes.com/2011/04/21/business/21data.html

20, 2011).[25] Ultimately, the company issued a correction. Press Release, Apple, Inc., Apple Q&A on Location Data (Apr. 27, 2011).[26]

During the 2011 holiday season, several malls decided to use shoppers' cell phones to track their movement from store to store. *See* Ken Wagstaff, *Will Your Mall Be Tracking Your Cellphone Today?*, Time (Nov. 25, 2011).[27] Experts noted that such a plan raised "a bunch of privacy red flags," Sean Gallagher, *We're Watching: Malls Track Shopper's Cell Phone Signals to Gather Marketing Data*, ArsTechnica (Nov. 2011).[28] Members of Congress also objected. *See* Press Release, U.S. Sen. Charles Schumer (Nov. 27, 2011).[29] Ultimately, the shopping centers involved decided against implementing the location tracking plans. Ashley Lutz, *Malls Cell-Phone Devices to Track Shoppers Halted After Complaints*, Bloomberg (Nov. 28, 2011).[30]

---

[25] *Available at* http://www.franken.senate.gov/files/letter/110420_Apple_Letter.pdf

[26] *Available at* https://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html

[27] *Available at* http://techland.time.com/2011/11/25/will-your-mall-be-tracking-your-cellphone-today/

[28] *Available at* http://arstechnica.com/business/news/2011/11/were-watching-malls-track-shoppers-cell-phone-signals-to-gather-marketing-data.ars.

[29] *Available at* http://schumer.senate.gov/Newsroom/record.cfm?id=334975.

[30] *Available at* http://mobile.bloomberg.com/news/2011-11-28/cell-phone-technology-to-track-shoppers-halted-after-complaints.

Consumers expect that information about their location will be used consistently with the context in which that information was collected. *See* Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2009); see also White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 15 (2012) ("Respect for context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."). In cases involving secret or unconsented location monitoring, this respect for context is violated, and thus, so are the reasonable privacy expectations of the individuals involved.

While the accuracy of location tracking varies depending on the density of cell base stations, consumers from both urban and rural environments have a legitimate expectation of location privacy. The use of new surveillance techniques should not prejudicially harm the privacy interests of the disadvantaged. As Judge Kozinski observed in a recent Ninth Circuit case concerning location tracking, "When you glide your BMW into your underground garage or behind an electric gate, you don't need to worry that somebody might attach a tracking device to it while you sleep. But the Constitution doesn't prefer the rich over the poor; the man who parks his car next to his trailer is entitled

to the same privacy and peace of mind as the man whose urban fortress is guarded by the Bel Air Patrol." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1123 (9th Cir. 2010) (Kozinski, J., dissenting). The privacy protection for the users of new communications services should not be dependent on one's wealth; courts should protect the privacy interests of all Americans.

B. In *United States v. Jones*, Five Justices Strongly Indicated that Location Tracking Violated a Reasonable Expectation of Privacy

Both Justice Sotomayor's and Justice Alito's concurring opinions in *United States v. Jones* suggested that the surreptitious tracking of an individual's location can infringe on an individual's reasonable expectation of privacy. *As* Justice Sotomayor explained, "In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention." *Jones*, 132 S. Ct. at 964 (Sotomayor, J., concurring). Justice Alito, writing for a four-member concurrence, said that the GPS monitoring in *Jones* "surely" violated society's expectations of privacy. *Id.* at 964 (Alito, J., concurring). Based on these two concurring opinions signed by five Justices, individuals have a reasonable expectation that the government will not use invasive techniques to track and store information about their location.

In discussing the degree of privacy that individuals reasonably expect in their location, both concurring opinions

focused on the unanticipated aspects of location tracking. Most people would not anticipate that such information is made easily available because previous conventional techniques used to monitor location contained inherent limitations that constrained their use: visibility and expense. *Id.* at 956 (Sotomayor, J., concurring). These details would have to be "take[n]. . . into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements." *Id.* at 956.

Similarly, Justice Alito noted that technological advances have enabled comprehensive, unprecedented levels of surveillance. "Perhaps [the] *most significant*" of these changes has been the ubiquity of cell phones, which "now permit wireless carriers to track and record the location of users," using cell phone towers or GPS. *Id.* at 963 (Alito, J., concurring) (emphasis added). Cell phones have made possible a level of surveillance that would have been impractical in the past: "The surveillance at issue in this case - constant monitoring of the location of a vehicle for four weeks - would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." *Id.* at 963. Thus, it involved "a degree of intrusion that a reasonable person would not have anticipated." *Id.* at 964.

C. Other Judicial Decisions Reflect an Increased Recognition of the Expectation of Privacy in an Individual's Location

The Supreme Court's opinion in *Jones* is the latest in a number of recent cases that reflect a growing recognition of the privacy interests that individuals have in their location data. Increasingly, courts have held both that cell phone users do not expect their location to be tracked while using a cell phone and that detailed location tracking infringes on a reasonable expectation of privacy.[31] Importantly, the resolution of this

[31] *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) (holding that probable cause was required to access historic CSLI under a variety of federal statutes governing law enforcement access to communications because, *inter alia*, "permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns . . . ."); *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, No. 10-2188-SKG, 2011 WL 3423370, at *9 (D. Md. Aug. 3, 2011) ("The Court finds that the subject here has a reasonable expectation of privacy both in his location as revealed by real-time location data and in his movement where his location is subject to continuous tracking over an extended period of time, here thirty days."); *In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) ("Compelled warrantless disclosure of cell site data violates the Fourth Amendment under the separate authorities of Karo and Maynard."); *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, No. 10-MC-0897 JO, 2010 WL 5437209, at *4 (E.D.N.Y. Dec. 23, 2010) (noting that "recent developments in pertinent case law have bolstered several different components of the analysis that previously led me to reject the government's reliance on the SCA to obtain records of a person's movements over a period of months without making a showing of probable cause.") *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) ("In light of drastic developments in technology, the Fourth Amendment

question appears to turn on the degree of precision allowed by the tracking practice at issue. For example, in 2010, the Third Circuit held that judges retain the option to impose a warrant requirement on law enforcement agents who seek location data but may choose to grant an order without a showing of probable cause. *In re Application of U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 319 (3d Cir. 2010). The court reached its decision because "[t]he record does not demonstrate whether [more precise tracking] can be accomplished with present technology, and we cannot predict the capabilities of future technology." *Id.* at 318. In contrast, subsequent opinions finding a reasonable expectation of privacy have relied heavily on the advancements in tracking technology. *See In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, No. 10-2188-SKG, 2011 WL 3423370, at *5 (D. Md. Aug. 3, 2011) ("Due to advances in technology and the proliferation of cellular infrastructure, cell-site location data can place a particular cellular telephone within a range approaching the accuracy of GPS."); *In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827(S.D. Tex. 2010) (denying application for location data after considering the detail

---

doctrine must evolve to preserve cell-phone user's reasonable expectation of privacy in cumulative cell-site-location records.").

available with GPS and cell site tracking and the prevalence of cell phones in modern society).

CONCLUSION

Amicus respectfully asks this Court to hold that the use of cell phone location tracking methods violates an individual's reasonable expectation of privacy because those methods are more invasive then the GPS tracking methods used in *United States v. Jones*, and judicial oversight is necessary to curb government abuse.