NO. 11-20884

IN THE
UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

IN RE: APPLICATIONS OF THE
UNITED STATES OF AMERICA
FOR HISTORICAL CELL-SITE DATA

On Appeal from the United States District Court
For the Southern District of Texas
Houston Division, Civil No. 4:11-MC-00223
Related Cases: 4:10-MJ-981, 4:10-MJ-990, 4:10-MJ-998

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER URGING AFFIRMANCE

Marc Rotenberg
Counsel of Record
John Verdi
Alan Butler
Electronic Privacy Information Center
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140

March 16, 2012

SUPPLEMENTAL STATEMENT OF INTERESTED PARTIES

Pursuant to Fed. R. App. P. 26.1 and 29(c), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judges of this court may evaluate possible disqualification or recusal.

The Electronic Privacy Information Center ("EPIC"), *amicus curiae*.

Marc Rotenberg
Counsel of Record
John Verdi
Alan Butler
Electronic Privacy Information Center
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

Jon Leibowitz, Chairman, Fed. Trade. Comm'n, Introductory Remarks at the FTC Privacy Roundtable (Dec. 7, 2009) 28

Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J.L. & Pol'y for Info. Soc'y 723 (2007) 30

Li B, Tan YK, Dempster AG, *Using Two Global Positioning System Satellites to Improve Wireless Fidelity Positioning Accuracy in Urban Canyons*, 5 IET Comm. 163 (2011) 13

MetroPCS, *Privacy Policy* 27, 31

Micah Sherr, et al., *Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps*, Proc. 16th ACM Conf. on Computer & Comms. Sec. 512 (Nov. 2009) 21, 22

Michael Benisch et al., *Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs*, 15 Personal & Ubiquitous Comp. 679 (2011) 25

Mike Y. Chen et al., *Practical Metropolitan-Scale Positioning for GSM Phones*, Ubicomp 225 (2006) 14

Nick Bilton, Tracking File Found in iPhones, N.Y. Times (Apr. 20, 2011) 26

Paul A Zandbergen, *Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning*, 13 Transactions GIS 5 (2009) 14

Press Release, Apple, Inc., Apple Q&A on Location Data (Apr. 27, 2011) 26

Press Release, Informa Telecoms & Media, The Shape of Mobile Networks Starts to Change as Femtocells Outnumber Macrocells in US (Oct. 21, 2010) 13, 14

Sprint Corporate Security: Electronic Surveillance Manual 21 (2002) 16

Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 26 Berkeley Tech. L.J. (forthcoming Mar. 2012) 9, 14, 16, 23

T-Mobile, *Privacy Policy* 27, 31

Transcript of Oral Argument, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259) 17

Verizon Wireless Law Enforcement Resource Team 25 (Apr. 20, 2009) 11

Vikram Chandrasekhar & Jeffrey G. Andrews, *Femtocell Networks: A Survey*, 46 Comm. Maga., IEEE 59 (2008) 12

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* in many cases before the U.S. Supreme Court and other courts concerning privacy issues, new technologies, and Constitutional interests. *See, e.g.*, *United States v. Jones*, 132 S. Ct. 945 (2012); *FAA v. Cooper*, 622 F.3d 1016 (9th Cir. 2010), *cert. granted* 131 S. Ct. 3025 (2011) (No. 10-1024); *First Am. v. Edwards*, 610 F.3d 514 (9th Cir. 2010), *cert. granted* 131 S. Ct. 3022 (2011) (No. 10-708); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011); *FCC v. AT&T Inc.*, 131 S. Ct. 1177 (2011); *NASA v. Nelson*, 131 S. Ct. 746 (2011); *Doe v. Reed*, 130 S. Ct. 2811 (2010); *Quon v. City of Ontario*, 130 S. Ct. 2619 (2010); *Tolentino v. New York*, 926 N.E.2d 1212 (N.Y. 2010), *cert. granted*, 131 S. Ct. 595, (2010) and *cert. dismissed as improvidently granted*, 131 S. Ct. 1387 (U.S. 2011); *Flores-Figueroa v. United States*, 129 S. Ct. 1886 (2009); *Herring v. United States*, 129 S. Ct. 695 (2009); *Crawford v. Marion Cnty. Election Bd.*, 128 S. Ct. 1610 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada*,

[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").

542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Dep't of Justice v. City of Chicago*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract Soc'y of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); *SEC v. Rajaratnam*, 622 F.3d 159 (2d Cir. 2010); *IMS Health v. Ayotte*, 550 F.3d 42 (1st Cir. 2008) *cert. denied*, 129 S. Ct. 2864 (2009); *Nat'l Cable and Telecomms. Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009); *Bunnell v. Motion Picture Ass'n of Am.*, No. 07-56640 (9th Cir. filed Nov. 12, 2007); *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); *Commonwealth v. Connolly*, 913 N.E.2d 356 (Mass. 2009); and *State v. Raines*, 857 A.2d 19 (Md. 2003).

EPIC has participated as *amicus curiae* in recent federal cases concerning constitutional privacy interests, including *United States v. Jones*, 132 S. Ct. 945 (2012); *Herring v. United States*, 129 S. Ct. 695 (2009); *Hepting v. AT&T*, 539 F.3d 1157 (9th Cir. 2008); *United States Telecomm. Ass'n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000).

EPIC has a particular interest in ensuring that Fourth Amendment privacy safeguards extend to location records in light of the Supreme Court's recent decision in *United States v. Jones*, 132 S. Ct. 945 (2012). Warrantless and suspicionless location tracking offends the right of individuals to maintain privacy

in their day-to-day activities, particularly when they would not reasonably expect such information to be gathered or made available to others.

SUMMARY OF THE ARGUMENT

The historical cell-site location data at issue in this case provides a comprehensive record of an individual's activities over a two-month period. This record is created by service providers and made available to the police without reasonable cause to believe that the individual is engaging in unlawful conduct. Customers neither knowingly nor voluntarily disclose this data to service providers. The data is generated automatically, without any affirmative act by the cell phone user. Users do not have an opportunity to control the type and amount of data collected; they do not even know what data is collected. If they were aware that such data existed, customers would reasonably assume that it is only used to enable cell phone service and disposed of when no longer needed. Customers reasonably expect that service providers do not generate and retain comprehensive records of their location without their knowledge or consent, and that any records stored will not be handed over to law enforcement without probable cause.

As this Court must now consider the legitimate privacy interests of users of new communication services, it bears emphasizing that cell phone tracking is precisely the type of activity that a majority of the Justices, writing in two separate concurrences in *United States v. Jones,* 132 S. Ct. 945 (2012), said would violate the reasonable expectation of privacy under the Fourth Amendment. Unlike the raw telephone numbers acquired by the police in *Smith v. Maryland,* 442 U.S. 735

(1979), the location data in historical cell-site records, of which consumers have no knowledge or understanding, crosses the line into a protected Fourth Amendment interest.

Following *Jones*, this Court should acknowledge individuals' reasonable expectation of privacy in months-long records of their locations and activities. The Court should protect individual privacy by holding the Government to a Fourth Amendment probable cause standard when it seeks to obtain comprehensive records concerning an individual's private activities.

ARGUMENT

An individual's day-to-day activities create a digital footprint that illustrates aspects of their social, political, professional, and personal identity. This is especially true of data generated by an individual's cell phone, which records with increasing accuracy where and when they have been, what they have done, and who they were with. The fact that this data travels over communications networks controlled by third parties does not change its sensitive and private nature. As Justice Sotomayor explained in *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring), the "premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" is an approach "ill suited to the digital age." *Id.* After all, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all." *Smith v. Maryland*, 442 U.S. 738, 749 (1979) (Marshall, J., dissenting).

When an individual cannot protect private information generated by her communications device, it is unreasonable to require her "to forgo use of what for many has become a personal or professional necessity" or else "accept the risk of surveillance." *Smith*, 442 U.S. at 750 (Marshall, J., dissenting). We should not "merely recite … risks without examining the desirability of saddling them upon society." *Id.* (citing *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting)). The majority opinion in *Smith* acknowledged that "where an

individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role …. [I]n such cases, a normative inquiry would be proper." *Smith*, 442 U.S. at 741 n.5.

This is such a case, and the court must now engage in that "normative inquiry" directly, and determine whether an individual has a justifiable and reasonable expectation in the privacy of their historical cell phone location records. Because five Supreme Court Justices writing in two separate concurrences in *Jones* concluded that month-long location tracking of a vehicle violated an individual's reasonable expectation of privacy, this court should hold that individuals have a reasonable expectation of privacy in two months of historical cell phone location records.

I. An Individual's Cell Phone Records Provide A Comprehensive History of The Person's Location

The Fourth Amendment protects individuals from government action that invades their "legitimate expectation of privacy." *Smith v. Maryland*, 442 U.S. 735, 740 (1979). Justice Alito, joined by four members of the court in *Jones*, analyzed whether "reasonable expectations of privacy were violated by the long-term monitoring of movements." *Jones*, 132 S. Ct. at 957 (Alito, J., concurring). He found that "the use of longer term GPS monitoring in investigations of most

offenses impinges on expectations of privacy." *Id.* Historical cell phone location records are uniquely invasive and the collection and use of cell-site data should be subject to the same strict Fourth Amendment considerations that apply to long-term GPS data. These records "emanat[e] from personal conduct" within constitutionally protected areas, and "reveal the most intimate details of a person's life." *Smith*, 442 U.S. at 747-48 (Stewart, J., dissenting).

In this case, the Government sought court orders to obtain sixty days of private location data from cell phone service providers. *See* Application at 2, *In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. Oct. 6, 2010) (No. 10-mj-00990). With this data, the Government can create a comprehensive map of a customer's movements, habits, relationships, and activities. Detailed records of an individual's movements over weeks and months are different in kind from the telephone number records discussed in *Smith*. This is no ordinary pen register or trap and trace device; it is a comprehensive profile of a person's private life.

The data requested by the Government would reveal, at a minimum, the location of the Target Device with sufficient accuracy to violate the customer's reasonable expectation of privacy. The historical record provided could also reveal a great deal more about the customer's movements, habits, religious affiliations and other intimate details of that individual's life than even the GPS data at issue in

Jones. In a world where people constantly carry their cell phones, "the greatest threat to privacy may not be snooping on people, but snooping on things" and "[t]he future of privacy will depend on a combination of legal and technical measures by which device-to-device communications are protected." Whitfield Diffie & Susan Landau, *Communications Surveillance: Privacy and Security at Risk*, 52 Comm. ACM 11 (2009).

A. Cell-Site Data Can Be Used to Pinpoint An Individual's Location With Increasing Accuracy, Down to A Room or Floor in a Building

Cell-site records already contain information about the location of the specific towers and tower sectors that users access throughout the day. Some records even estimate the user's distance from the tower. As technology improves, these historical location records will provide an increasingly accurate portrait of the user's day-to-day activities. *See generally* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 26 Berkeley Tech. L.J. (forthcoming Mar. 2012). Cellular technology works by connecting mobile phones to the service provider's network through a system of radio base stations ("cell sites"). When a customer sends or receives a call or text message, or accesses the Internet, the wireless service provider automatically logs the call detail information. *See* Computer Crime & Intellectual Property Section, Dept. of

Justice, *Retention Periods of Major Cellular Service Providers* (Aug. 2010).[2] These logs typically contain a wide range of information, including:

- The date the call was made
- The time the call was made
- The duration of the call
- The identity of the subscriber's device
- The identity of the service provider
- The identity of the switch used to route the call
- The identity of the cell tower used to access the switch
- The 'sector' of the antenna used to access the cell tower

See Application at 2-3, *In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. Oct. 6, 2010) (No. 10-mj-00990).[3]

Some carriers record not only the cell-site location, but also the caller's estimated distance from the tower, pinpointing the user's location with even

[2] *Available at* http://www.wired.com/images_blogs/threatlevel/2011/09/retentionpolicy.pdf.

[3] The records sought by the Government in this case include, at a minimum, historical cell-site data, which is created automatically during the everyday use of a cell phone. As the Government describes in its application:

> A cell phone must send a radio signal to an antenna tower which, in turn, is connected to the provider's network. The area covered by the tower varies depending on the population density of the area. This area is often divided into thirds—120 degree sectors. "Cell site information" as used in this application refers to the antenna tower and sector to which the cell phone sends its signal. This includes the physical location and/or address of the cellular tower and identification of the particular sector of the tower receiving the signal.

Application at 2 n.3, *In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d 827.

greater accuracy. For example, a sample Verizon call detail table provides law enforcement with access to not only time, date, call length, and cell-site location and sector, but also the subscriber's distance in miles from the cell site. Records are created whenever a call begins or ends.

Date *	Access Time	Call End Time *	Call Length (sec)	ESN	Subscriber #	Entry Type *	Init Cell	Init Sector	Access Dist (mi)	Last Cell	Last Sector
4-Apr	53:50.3	54:55.7	65.4	1438dac0	9084488669	Term	168	3	1.1	106	1
2-Apr	27:54.2	29:11.8	77.6	1438dac0	9084488669	Orig	292	2	0	292	2
1-Apr	25:42.5	26:44.8	62.4	1438dac0	9084488669	Orig	293	1	0.3	293	2
1-Apr	24:52.7	25:18.5	25.9	1438dac0	9084488669	Term	293	1	0.8	293	1
31-Mar	38:13.6	38:39.4	25.8	1438dac0	9084488669	Term	138	1	0.6	138	1
31-Mar	02:06.8	03:05.8	59	1438dac0	9084488669	Orig	14	1	0.8	14	1
31-Mar	20:24.7	20:31.6	7	1438dac0	9084488669	Orig	3	1	1.9	3	1
31-Mar	52:35.5	01:35.4	539.9	1438dac0	9084488669	Orig	138	1	0.6	138	1

Fig. 1. Sample Historical Cell Site Location Information.

Verizon Wireless Law Enforcement Resource Team 25 (Apr. 20, 2009).[4] In this sample data, a suspect's distance is revealed to within .1 of a mile.

In dense urban areas there can be hundreds of cell towers and antennae packed into a few city blocks.[5] Low-density areas where cell sites are far apart, or impeded by terrain and position, and cannot accurately track a user's location, are

[4] *Available at* http://publicintelligence.net/verizon-wireless-law-enforcement-resource-team-lert-guide/. This table uses the round trip transmission time in calculating the user's approximate distance from the cell site, a technique which is available for recently completed calls. *See Wireless Carrier Policies for Exigent Situations*, NINA 2010 9-1-1 Conf. & Trade Show 12 (June 8, 2010), *available at* http://www.michigan.gov/documents/msp/Wireless_Carrier_Policies_for_Exigent_Situations_NENA_FINAL_325433_7.pdf.

[5] A quick search of the area surrounding the Court of Appeals for the Fifth Circuit Courthouse, 600 S. Maestri Place, New Orleans, LA 70130-3408, reveals more than two hundred antenna sites and fifty towers in a two-mile radius. Search tools based on publicly available information are available at http://www.antennasearch.com based on publicly available information. For a map of the antennae around the courthouse see http://epic.org/amicus/location/cell-phone-tracking/NOLA-antennae.html and for towers see http://epic.org/amicus/location/cell-phone-tracking/NOLA-towers.html.

outliers in the general trend of universal coverage for cell phones.[6] This trend towards denser cell-site placement has accelerated with the popularity of smartphones. The typical smartphone user consumed thirty-five times more mobile bandwidth in 2011 than the user of a basic-feature cell phone. Cisco, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015* (2012). As smartphone use continues to grow, service providers will need to build more cell sites to keep up with the increased data traffic. John M. Chapin & William H. Lehr, *Mobile Broadband Growth, Spectrum Scarcity, and Sustainable Competition*, 39th Res. Conf. on Comm., Info. & Internet Pol'y (Sept. 23, 2011).[7]

In addition to conventional high-power cell sites, carriers also use femtocells to route calls between consumers and the cellular network. Femtocells are "short range, low cost and low power base-stations, installed by the consumer." Vikram Chandrasekhar & Jeffrey G. Andrews, *Femtocell Networks: A Survey*, 46 Comm. Maga., IEEE 59 (2008). They free up spectrum and provide better coverage and data rates at a low cost, helping to meet data traffic needs of smartphones. *See id.* Femtocells are now available to general users of several cellular providers. *See,*

---

[6] If the court finds the location records in this case were "generalized" and not private because the particular cell sites used were too far apart to create an accurate record, that decision should be limited to the unique facts of this case. *See In re Application of U.S. for an Order for Disclosure of Telecomms. Records and Authorizing the Use of a Pen Register and Trap and Trade Device*, 405 F. Supp. 2d 435, 450 (S.D.N.Y 2005) (noting that whether an area was "densely populated by cell towers" was a factor in authorizing law enforcement access to the cell-site data).

[7] *Available at* http://people.csail.mit.edu/wlehr/Lehr-Papers_files/chapin_lehr_tprc2011%20mobile%20broadband.pdf.

e.g., *AT&T 3G Microcell – Wireless Signal Booster*, AT&T (last visited Mar. 6, 2012).[8] Femtocells have a range of approximately ten meters. *See, e.g.*, *id.* ("What is the range of the AT&T 3G MicroCell device? The signal range is approximately 40 feet from the base station (in all directions), or about 5000 square feet."). Thus, connection data from a single femtocell can provide more accurate location information than GPS data, especially since GPS measurements are inaccurate indoors or in large cities where buildings create "urban canyons." Li B, Tan YK, Dempster AG, *Using Two Global Positioning System Satellites to Improve Wireless Fidelity Positioning Accuracy in Urban Canyons*, 5 IET Comm. 163 (2011).

Cellular carriers increasingly rely on femtocells. In the United States, femtocells now outnumber conventional cell sites. Press Release, Informa Telecoms & Media, The Shape of Mobile Networks Starts to Change as Femtocells Outnumber Macrocells in US (Oct. 21, 2010),[9] ("Conservative estimates suggest there are currently 350,000 femtocells and around 256,000 [conventional cell sites] in the U.S. Furthermore by March 2011, there are expected to be at least twice as many femtocells as [conventional cell sites] in the U.S."). And the number of femtocells is growing rapidly. Experts estimate that by 2016 femtocells will

[8] http://www.att.com/shop/wireless/devices/3gmicrocell.jsp.
[9] *Available at* www.smallcellforum.org/pressreleases.php?id=269.

constitute 88% of all cell sites globally. *Id.* As time passes, cell-site data will reveal increasingly more accurate location information about cell phone users.

Some carriers routinely record even more accurate data about customer location by triangulating the phone's longitude and latitude. The use of these network-based location methods allow carriers to pinpoint a customer's location to within fifty meters. Paul A Zandbergen, *Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning*, 13 Transactions GIS 5, 11 (2009) ("Horizontal error . . . var[ies] greatly across urban-rural gradients, with a median error in the order of 50 to several hundred meters in urban areas and in the order or [sic] several hundred meters to several kilometers in rural areas.").[10] While not all carriers currently do this, "movement towards this practice is a general trend in the industry." Stephanie K. Pell & Christopher Soghoian, *supra*, at 11.

B. Cell Phones Are Ubiquitous in the United States and Cell-Site Records Are Continuously Updated Throughout Each Day

The collection of cell-site data allows law enforcement to track an individual's location over many weeks or months retroactively. The growing divergence between the customer's expectation of privacy and law enforcement

[10] A separate study found location from cell-site data could be calculated with a median error of 94m in urban areas (66 cell sites per km^2) and 196m in residential areas (26 cell sites per km^2). Mike Y. Chen et al., *Practical Metropolitan-Scale Positioning for GSM Phones*, Ubicomp 225 (2006). Since 2006, the number of cell tower sites in the United States has increased from 197,576 to more than 256,920. *See* CTIA: The Wireless Association, *Wireless Quick Facts*, http://www.ctia.org/advocacy/research/index.cfm/aid/10323 (last visited Mar. 14, 2012).

cell phone tracking is underscored by the prevalence and importance of cell phones in everyday life. A recent study shows that 88% of American adults own a cell phone. Aaron Smith, *46% of American Adults Are Smartphone Owners*, Pew Research Center at 2 (Mar. 1, 2012).[11] A majority of these cell phone users now own smartphones. *Id*. Cell phone users make or receive "an average of 12 calls on their cells per day." Aaron Smith, *31% of Text Message Users Prefer Texting to Voice Calls, and Young Adults Stand Out In Their Use of Text Messaging*, Pew Research Center at 2 (Sept. 19, 2011).[12] About three-fourths of cell phone owners send and receive text messages. *Id.* The average text message user sends or receives 41.5 messages per day. *Id*. For young adults, texting is even more prevalent, with the average user between the ages of 18 and 24 exchanging more than 100 messages per day, or 3,200 per month. *Id*. Every message and call creates a new entry in the user's historical location record.

Cell phone use is not limited to sending and receiving voice and text messages. The majority of adult cell phone owners now have smartphones and use them to find help in emergencies, to quickly retrieve useful information, to stave off boredom, to share social experiences with friends near and far, and even to "prevent unwanted personal interactions." Aaron Smith, *Mobile Devices Help*

[11] http://www.pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf.

[12] http://pewinternet.org/~/media//Files/Reports/2011/Americans%20and%20Text%20Messaging.pdf.

People Solve Problems and Stave Off Boredom, But Create Some New Challenges and Annoyances, Pew Research Center at 2 (Aug. 14, 2011).[13] Cell phones truly are a "near-ubiquitous tool for information-seeking and communicating." *Id.* Besides texting and chatting, more than 50% of all cell phone owners use their devices to send photos or videos, and nearly 50% use their devices to access the Internet. *Id.* More than 80% of smartphone owners use these functions. *Id.* at 7.[14] Americans carry their cell phones with them everywhere, all day, every day. The devices are increasingly intertwined with their social, political, professional, and educational lives. Every time individuals use their devices, a record is created. Stephanie K. Pell & Christopher Soghoian, *supra*, at 21 (describing carrier records for recently placed calls and text messages); *Sprint Corporate Security: Electronic Surveillance Manual* 21 (2002) (including "web browsing" on the list of call types).[15]

The historical records maintained by service providers are truly comprehensive, showing the cell phone's location updated continuously during the day as the user goes from home, to work, to school, to church and to other private locations. These records are even more comprehensive than the GPS records in

[13] http://www.pewinternet.org/~/media//Files/Reports/2011/Cell%20Phones%202011.pdf.
[14] For smartphone owners: 92% send or receive text messages, 84% access the internet, 80% send or receive photo or video, and 76% send or receive e-mail. Aaron Smith, *Americans and Their Cell Phones*, Pew Research Center at 7 (Aug. 14, 2011).
[15] *Available at* http://cryptome.org/isp-spy/sprint-spy.zip.

Jones. The Court in *Jones* discussed the difference between tracking cars and tracking individuals:

> JUSTICE KENNEDY: Well, under that rationale, could you put a beeper surreptitiously on the man's overcoat or sport coat?
>
> MR. DREEBEN: Probably not, Justice Kennedy; and the reason is that this Court in *Karo v. United States* -- *United States v. Karo* -- specifically distinguished the possibility of following a car on a public roadways from determining the location of an object in a place where a person has a reasonable expectation of privacy.

See Transcript of Oral Argument at 5, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259). The average cell phone user sends or receives calls, text messages, or Internet data more than fifty times per day. Smartphone owners use their devices for on-going tasks like e-mail,[16] which require frequent connections as the phone contacts an e-mail server every few minutes to check for new messages. All of these connections generate location data. This location record creates a comprehensive map of an individual's movements, activities, and relationships over the course of many weeks and months. This is precisely the type of information that individuals reasonably and justifiably believe will remain private, like the record at issue in *Jones*.

[16] According to a recent Pew Internet study, 76% of smartphone users send or receive e-mail on their phones. Aaron Smith, *Americans and Their Cell Phones*, Pew Research Center at 3 (Aug. 15, 2011), http://www.pewinternet.org/~/media//Files/Reports/2011/Cell%20Phones%202011.pdf.

II. The Third Party Doctrine Is Inapplicable In This Case Because Cell Phone Location Data Is Automatically Generated Without Users' Knowledge Or Consent

It cannot be said that a user's "reasonable understanding" of cell phone technology and industry practices includes knowledge of, and consent to, constant location tracking by the government without probable cause. All empirical research points to the opposite conclusion: as devices become more complex, and as cell phone service privacy policies stretch on to many pages, customers understand less, not more, about how their devices work. The records at issue here are not like the telephone numbers in *Smith*, which the users dialed. Rather, the data is generated automatically without user knowledge or control. The amount of data generated by the average cell phone is constantly increasing as devices evolve and new functions emerge. The devices are now so complex that the average user does not understand how they function. According to a study, 14% of cell phone users do not even know whether their phone is a smartphone. Aaron Smith, *35% of American Adults Own a Smartphone*, Pew Research Center at 5 (July 7, 2011).[17]

Furthermore, users have no control over the type or amount of private data collected by cellular service providers. Federal telecommunications laws require providers to implement particular technologies and standards in their networks that enable easy compliance with prospective law enforcement intercept and call detail

[17] http://pewinternet.org/~/media/Files/Reports/2011/PIP_Smartphones.pdf.

requests. These laws require that all carriers implement a specific network architecture, so customers have no meaningful opportunity to choose even if they were knowledgeable about the existence of automatic location records. Customers and service providers have about as much choice in the content and volume of these records as they do in the format and content of their tax documents. Furthermore, the disclosure of historical location records is "not entirely volitional" because a cell phone is now a necessity for the average American.

"Implicit in the concept of assumption of risk is some notion of choice." *Smith v. Maryland*, 442 U.S. at 749 (Marshall, J., dissenting). It cannot be reasonably said that users "assumed the risk" of disclosure to the government where the records at issue are generated automatically, without the user's knowledge. Fourth Amendment protections should not turn on "concededly 'esoteric functions' … [of] which subscribers are unlikely to have intimate familiarity." *Id.* at 749 n.1. At the time Justice Marshall drafted his dissenting opinion in *Smith*, there was only one telephone provider and the most exciting recent developments in telephone technology were keypad dialing, customer long distance dialing, and electronic call switching. *See* AT&T, *Milestones in AT&T History*.[18] Today the average American has more than five available facilities-based cell phone service providers, and more than six hundred and thirty different

[18] http://www.corp.att.com/history/milestones.html (last visited Mar. 13, 2012).

handsets, to choose from. CTIA: The Wireless Association, *The Wireless Industry Facts: An Independent Review* (Aug. 2010).[19] Each of these providers uses a different technology and stores different data about their customers. Even if a cell phone user was willing and able to understand the type and amount of data generated by their phone, they would have no way to learn what data their device creates, or what data their provider stores.

A. Service Providers Configure Telephone Systems To Automatically Generate Cell-Site Data In Order to Comply With Federal Wiretap Laws, a Purpose Unrelated to the Delivery of Cellphone Service

The Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), 18 U.S.C. §§ 1001-1010, requires "telecommunications carriers to ensure that their systems are technically capable of enabling law enforcement agencies operating with proper legal authority to intercept individual telephone calls and to obtain 'call-identifying information.'" *U.S. Telecomm. Ass'n v. FCC*, 227 F.3d 450, 453 (D.C. Cir. 2000). The CALEA was enacted to "preserve the government's ability … to intercept communications involving advanced technologies," H.R. Rep. No. 103-827, pt. 1, at 9 (1994), and it did so by requiring service providers to build intercept capabilities into their networks. *U.S. Telecomm. Ass'n*, 227 F.3d at 454. These capabilities are described in an industry standard, the

[19] http://files.ctia.org/pdf/082010_Independent_Assessment_of_Wireless_Industry.pdf.

"J-Standard,"[20] adopted by the Telecommunications Industry Association ("TIA") in accordance with FBI negotiations. *Id.* at 455. Under the CALEA safe harbor provision, "carriers that comply with the accepted [standard] will be deemed in compliance with the statute." *See* 47 U.S.C. § 1006(a)(2).

The J-Standard, created and adopted in response to CALEA's compliance mandate, dictates the default network architecture of every cell phone service provider (and other telecommunications service provider) in the United States. *See* Micah Sherr, et al., *Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps*, Proc. 16th ACM Conf. on Computer & Comms. Sec. 512, 514 (Nov. 2009) ("This architecture is the only currently fielded standard for complying with CALEA.").[21] "The J-standard mandates that some or all network elements be able to function as *interception access points* (IAPs) when authorized by a wiretap order." *Id.* Under the standard, the provider's network must be able to interface with a law enforcement "collection function" on request. *Id.* at 515. "Call-identifying information is transmitted using the *Lawfully Authorized Electronic Surveillance Protocol* (LAESP), a message-based protocol that encodes actions taken by the TSP or the wiretap subject." *Id.* Each message "must contain (at a minimum) a timestamp, a case identifier, and possibly the identity of the IAP

[20] American National Standards Institute, *Lawfully Authorized Electronic Surveillance*, Joint Standard ANSI/J-STD/025B, TIA/ATIS, Aug. 2003.
[21] *Available at* http://www.crypto.com/papers/calea-ccs2009.pdf.

that intercepted the call-identifying information." *Id.* at 517. The J-standard also covers text message "services such as the Short Message Service (SMS)." *Id.*

As a result of the implementation and acceptance of the J-Standard, cell phone users have no opportunity to switch providers or otherwise escape the tracking-enabled network architecture. These cell phone networks automatically create location records, which can be forwarded to law enforcement in real time "pursuant to a court order or other lawful authorization," 47 U.S.C. § 1002(a)(1), or stored over the long term. But carriers must also facilitate access to these records "in a manner that protects … the privacy and security of communications and call-identifying information not authorized to be intercepted." *Id.* at §1002(a)(4)(A). The CALEA creates a system that gives consumers no choice in the network architecture of their communications providers, but it expressly grants privacy protections for sensitive records. Thus the CALEA both underscores the lack of voluntariness and consent to collection of these records, and reinforces the expectation that when personal information is collected, it will remain private.

After the J-Standard was first adopted and implemented by an order of the Federal Communications Commission ("FCC"), it was challenged on the grounds that it "impermissibly expanded the types of call-identifying information that carriers must make accessible" to include antenna tower location information. *U.S. Telecomm Ass'n*, 227 F.3d at 453. The Court of Appeals for the District of

Columbia Circuit upheld portions of the J-Standard that included location information within the "call-identifying information" protocol, noting that Section 103(a)(2) of CALEA explicitly limits the disclosure of "physical location of the subscriber" as part of call-identifying information "acquired solely pursuant to the authority for pen registers and trap and trace devices." *Id.* at 463 (citing 47 U.S.C. § 1002(a)(2)). The Court emphasized that "[t]he Commission demonstrated its understanding that antenna location information could only be obtained with something more than a pen register order … a point the Justice Department concedes in its brief: 'A pen register order does not by itself provide law enforcement with authority to obtain location information, and we have never contended otherwise.'" *Id.* at 464. Even the FCC noted when it adopted the J-Standard that precise location tracking "could undermine individual privacy." Communications Assistance for Law Enforcement Act, 14 FCC Rcd. 16794 at ¶ 46 (1999) ("Third Report and Order").

The Government now commonly orders service providers to turn over historical location records in response to a "hybrid" pen register order. *See* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 26 Berkeley Tech. L.J. (forthcoming Mar. 2012). The Government requires that service providers gather this location data automatically

in case it gets a warrant, then applies for an order under the minimal pen register standard after that data is stored, even though it already conceded that such a minimal standard was insufficient to justify collection of location data in the first place. *See U.S. Telecomm Ass'n*, 227 F.3d at 464.

Given that the government itself first mandated the collection of this data, it cannot reasonably argue that disclosure of the data is voluntary in any meaningful sense when it attempts to obtain private location records. This point alone clearly distinguishes the matter before the court from *Smith v. Maryland.* 442 U.S. at 749 (Marshall, J., dissenting) ("It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.").

B. Cell Phone Users Reasonably Expect That Their Location Data Will Not Be Disclosed During Normal Cell Phone Use

Cell phones and other consumer electronic devices generate enormous amounts of location data, and the collection and use of this data often occurs without the user's knowledge or consent. A recent survey found that 77% 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).[22] Other surveys found that although some users are aware that cell phones disclose location data to application developers, they are concerned about controlling who has access to their location. Janice Y. Tsai et al., *Location-Sharing*

[22] http://www.scribd.com/doc/54220855/TRUSTe-Mobile-Privacy-Report.

Technologies: Privacy Risks and Controls (2010).[23] A study conducted by Microsoft researchers found that individuals were concerned about access to location data, "strongly agree[ing] that companies should never share personal information unless it has been authorized by the individual." A.J. Bernheim Brush et al., *Exploring End User Preferences for Location Obfuscation, Location-Based Services, and the Value of Location*, Proc. UbiComp 95, 99 (Sept. 2010). The study participants were generally only willing to share or publicize this data if effective anonymization and obfuscation techniques were in place to address their privacy concerns. *Id.* at 101.

Another study conducted by Carnegie Mellon University researchers in 2009 demonstrated that mobile phone users have "rich location-privacy preferences" and want control over the collection and sharing of their location data with third parties in fine granularity along several dimensions, including time of day, day of week, and by location. Michael Benisch et al., *Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs*, 15 Personal & Ubiquitous Comp. 679 (2011).

These findings are corroborated outside of an academic context. 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

[23] *Available at* http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

Blog: Wheels (Sept. 22, 2011).[24] 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.[25] Consumers were very upset when they learned of this, and ultimately, the company revised the operating system to correct the problem. Press Release, Apple, Inc., Apple Q&A on Location Data (Apr. 27, 2011).[26]

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 individuals' reasonable privacy expectations.

[24] http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users.
[25] *Available at* https://www.nytimes.com/2011/04/21/business/21data.html
[26] *Available at* https://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html

C. The Mere Existence of a Privacy Policy Does Not Eliminate a Cell Phone User's Reasonable Expectation That Their Location Data Will Remain Private

In this case, the Government applied for "hybrid" orders to obtain the historical location records of MetroPCS and T-Mobile customers. Both MetroPCS and T-Mobile have extensive privacy policies available via the Internet, separate from the service contracts signed by users when they register for a cell phone. These privacy policies discuss the location data automatically stored by their networks.[27] However, these online statements are not evidence that consumers reasonably understand or voluntarily convey their location information in a way that eliminates their Fourth Amendment expectation of privacy. The customers here may have had no reason or opportunity to read these online statements. Even where customers are aware of these policies, comprehensive empirical studies reveal that users rarely read them, and instead assume privacy policies assure that their information is protected. *See* discussion *infra* pp. 28-31. The mere existence of such policies does not indicate that customers have "assumed the risk of disclosure."

[27] *See* MetroPCS, *Privacy Policy*, http://www.metropcs.com/metro/tac/termsAndConditions.jsp?terms=Terms%20and%20Conditions%20of%20Service (last visited Mar. 13, 2012); T-Mobile, *Privacy Policy*, http://www.t-mobile.com/company/website/privacypolicy.aspx (last visited Mar. 13, 2012). The total word count of these privacy policies combined is 8,891, which is 1,891 more than the maximum allowable word count for this amicus curiae brief.

Privacy researchers have found that users rarely read privacy policies. *See, e.g.*, Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 Info. Sys. Research 254, 256 (2011) (citing *Consumers Have a False Sense of Security About Online Privacy: Actions Inconsistent with Attitudes*, TRUSTe, Dec. 2006;[28] Carlos Jensen et al., *Privacy Practices of Internet Users: Self-reports Versus Observed Behavior*, 63 Int'l J. Human-Computer Studies 203, 223 (2005) ("[O]nly a minority of subjects read policies with any frequency.")).

Even senior government officials, charged with consumer protection, have publically acknowledged that users do not read privacy policies. "We all agree that consumers don't read privacy policies – or EULAs, for that matter." Jon Leibowitz, Chairman, Fed. Trade. Comm'n, Introductory Remarks at the FTC Privacy Roundtable (Dec. 7, 2009).[29] Similarly, David Vladeck, the Director of the FTC's Bureau of Consumer Protection told the New York Times that: "… I don't believe that most consumers either read [privacy disclosures], or, if they read them, really understand it." Stephanie Clifford, *An Interview With David Vladeck of the F.T.C.*, N.Y. Times Blog: Media Decoder (Aug. 5, 2009).[30] Even Chief Justice

[28] http://www.prnewswire.com/news-releases/consumers-have-false-sense-of-security-about-online-privacy---actions-inconsistent-with-attitudes-55969467.html.
[29] *Available at* http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf.
[30] http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/.

Roberts admitted that he doesn't usually read the terms of service or privacy policies:

> It has "the smallest type you can imagine and you unfold it like a map," he said. "It is a problem," he added, "because the legal system obviously is to blame for that." Providing too much information defeats the purpose of disclosure, since no one reads it, he said. "What the answer is," he said, "I don't know."

Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, A.B.A. J. (Oct. 20, 2010).[31]

Many recent empirical studies have addressed the question of whether individuals read contracts, especially online licenses and policies. *See generally* Zev J. Eigen, *Empirical Studies of Contract*, Ann. Rev. L. & Soc. Sci. (forthcoming 2012) (manuscript at 6, 8, 15-16).[32] As Professor Eigen's review of recent research describes, these studies find that individuals tend not to read form contracts or boilerplate language like that contained in the privacy policies at issue here. *Id*. at 15. In one study, a New York University research group monitored the Internet browsing behavior of over 45,000 users. An analysis of the data revealed that the "average rate of readership of [online licensing agreements] is on the order of 0.1 percent to 1 percent," which included everyone who accessed the licensing webpage for at least one second. Florencia Marotta-Wurgler, *Will Increased*

[31] http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print/.
[32] *Available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1998483.

Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts," 78 U. Chi. L. Rev. 165, 168 (2011).

The Samuelson Clinic at the University of California, Berkeley found that only 1.4 percent of 222 study participants reported reading license agreements often and thoroughly. By contrast, 66.2 percent reported rarely reading or browsing the contents of EULAs, and 7.7 percent said they had never noticed these agreements or had never read them. Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J.L. & Pol'y for Info. Soc'y 723, 740 (2007).[33]

It should be no surprise that users routinely ignore privacy policies. As a Carnegie Mellon research team recently calculated, it would take an average consumer approximately 200 hours each year to read the privacy policies of all of the sites they visited, with annual costs of about $3,534. The researchers concluded that, "[n]ationally, if Americans were to read online privacy policies word-for-word, we estimate the value of time lost as about $781 billion annually." Aleecia M. McDonald, *Footprints Near the Surf: Individual Privacy Decisions in Online Contexts* 11-28 (Dec. 1, 2010) (unpublished Ph.D dissertation, Carnegie Mellon

[33] *Available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/FTC_and_privacy.pdf.

Univ.);[34] Aleecia McDonald & Lorrie Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & Pol'y for Info. Soc'y 543 (2008).[35]

Even when users do read privacy policies, they are likely to be confused or to assume that their rights are being protected, rather than the opposite. The privacy policies in this case indicate that location records are created automatically to route and complete wireless calls. *See generally* Brief for the United States at 20-21. However, these policies also make clear that "[u]nder federal law, you have a right, and we have a duty, to protect the confidentiality of [Consumer Proprietary Network Information]," which includes "call location information." T-Mobile, *Privacy Policy*.[36] The existence of these privacy policies does not establish consumer knowledge of or consent to disclosure of historical location records. In fact, if a customer did read these policies, they would likely believe that the "confidentiality" of their location data was assured.

CONCLUSION

Amicus respectfully asks this Court to hold that the Government cannot obtain historical cell-site data without probable cause because individuals have a

[34] *Available at* http://repository.cmu.edu/dissertations/7/.
[35] *Available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.
[36] http://www.t-mobile.com/company/website/privacypolicy.aspx (last visited Mar. 13, 2012). MetroPCS, Privacy Policy, http://www.metropcs.com/metro/tac/termsAndConditions.jsp?terms=Privacy%20Policy ("We have a duty, to protect the confidentiality of information about … the location of your device on our network when you make a voice call.") (last visited Mar. 13, 2012).

reasonable expectation of privacy in their cell phone location records and do not voluntarily disclose that data in a way that waives their privacy interest.

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(B)(i). This brief contains 6,913 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5); 5th Cir. R. 32.2 and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word in 14 point Times New Roman style.

Dated: March 16, 2012

___*/s/ Marc Rotenberg*_____
Marc Rotenberg
Counsel of Record
John Verdi
Alan Butler
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on this 16th day of March, 2012, the foregoing Brief of *Amicus Curiae* was electronically filed with the Clerk of the Court, and thereby electronically serve upon counsel for the parties *via* electronic delivery. Also, EPIC sent 2 copies to each party via U.S. Mail, postage prepaid, on March 16, 2012.

Dated: March 16, 2012

/s/ Marc Rotenberg
Marc Rotenberg
Counsel of Record
John Verdi
Alan Butler
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140