12-4659; 12-4825

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff–Appellee,

v.

AARON GRAHAM and ERIC JORDAN,

Defendants–Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND, NORTHERN DIVISION

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND, CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, & NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF DEFENDANTS-APPELLANTS AND REVERSAL

Nathan Freed Wessler
Catherine Crump
Ben Wizner
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500

David R. Rocah
American Civil Liberties Union Foundation of Maryland
3600 Clipper Mill Road, Suite 350
Baltimore, MD 21211
(410) 889-8555

Kevin S. Bankston
Gregory T. Nojeim
Center for Democracy & Technology
1634 I St NW, Suite 1100
Washington, DC 20006
(202) 637-9800

Hanni Fakhoury
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Thomas K. Maher
Vice-Chair, 4th Circuit
Amicus Committee
National Association of Criminal
Defense Lawyers
123 W. Main St.
Suite 400
Durham, NC 27701
(919) 354-7200

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union Foundation ("ACLU") is a nationwide, non-profit, non-partisan public interest organization of more than 500,000 members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU Foundation of Maryland, the organization's affiliate in Maryland, was founded in 1931 to protect and advance civil rights and civil liberties in that state, and currently has approximately 14,000 members. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to both organizations. The ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy.

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

---

[1] Pursuant to Rule 29(a), counsel for *amici curiae* certifies that all parties have consented to the filing of this brief. Pursuant to Rule 29(c)(5), counsel for *amici curiae* states that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported organization based in San Francisco, California, that works to protect privacy and free speech rights in an age of increasingly sophisticated technology. As part of that mission, EFF has served as counsel or *amicus curiae* in many cases addressing Fourth Amendment issues raised by emerging technologies, including location-based tracking techniques such as GPS and collection of cell site tracking data. *See, e.g.*, *United States v. Jones*, 132 S. Ct. 945 (2012), *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010); *United States v. Jones*, 908 F. Supp. 2d 203 (D.D.C. 2012); *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010), *Commonwealth v. Rousseau*, --- N.E.2d ----, 465 Mass. 372 (2013).

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of approximately 10,000 direct members in 28 countries, and 90 state, provincial and local affiliate organizations totaling up to 40,000 attorneys. NACDL's members include private criminal defense lawyers, public defenders, military defense

counsel, law professors, and judges. NACDL files numerous amicus briefs each year in the Supreme Court, this Court, and other courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

SUMMARY OF ARGUMENT

Location surveillance, particularly over a long period of time, can reveal a great deal about a person. "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 sub nom. United States v. Jones*, 132 S. Ct. 945 (2012). Accordingly, in *United States v. Jones*, five Justices of the Supreme Court concluded that an investigative subject's "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." 132 S. Ct. at 958, 964 (Alito, J. concurring in the judgment); *id.* at 955 (Sotomayor, J. concurring).

In this case, law enforcement obtained 221 days of cell site location information ("CSLI") for each defendant's phone without a warrant. If tracking a vehicle for 28 days in *Jones* was a search, then surely tracking a cell phone for 221 days is likewise a search, particularly because people keep their phones with them as they enter private spaces traditionally protected by the Fourth Amendment.

The district court distinguished *Jones*, but its reasoning rests on an unjustifiably narrow reading of that case because it fails to take account of five Justices' determination that Americans have a reasonable expectation that they will

not be subject to long-term and constant surveillance of their movements. The district court's reliance on Supreme Court jurisprudence regarding bank records and dialed telephone numbers is similarly misplaced, because cell phone location data is not voluntarily communicated to phone service providers, in contrast to the willful communication of banking transaction data and dialed numbers to banks and telecommunication companies. The government's acquisition of Defendants' comprehensive cell phone location information without a warrant violates the Fourth Amendment.

ARGUMENT

I. WARRANTLESS ACQUISITION OF LONG-TERM HISTORICAL CELL SITE LOCATION INFORMATION VIOLATED DEFENDANTS' REASONABLE EXPECTATION OF PRIVACY UNDER THE FOURTH AMENDMENT.

A. Defendants' Cell Site Location Information Obtained by the Government Reveals Invasive and Accurate Information About Their Location and Movements Over Time.

i. Cell site location information reveals private, invasive, and increasingly precise information about individuals' locations and movements.

As of December 2012, there were 326.4 million wireless subscriber accounts in the United States, responsible for 2.30 trillion annual minutes of calls and 2.19 trillion annual text messages.[2] Cell phone use has become ubiquitous: the number

[2] *U.S. Wireless Quick Facts*, CTIA – The Wireless Association, *available at* http://www.ctia.org/advocacy/research/index.cfm/aid/10323.

of wireless accounts now exceeds the total population of the United States,[3] more than 83% of American adults own cell phones,[4] and one in three U.S. households has only wireless telephones.[5]

Cellular telephones regularly communicate with the carrier's network by sending radio signals to nearby base stations, or "cell sites." *The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. on the Judiciary* 113th Cong. 6 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania)[6] ["Blaze Hearing Statement"]. When turned on, "[c]ell phone handsets periodically (and automatically) identify themselves to the nearest base station (that with the strongest radio signal) as they move about the coverage area." *Id.* Phones communicate with the wireless network when a subscriber makes or receives calls or transmits or receives text messages. Smartphones, which are now used by more

---

[3] *Id.*
[4] Aaron Smith, Pew Research Ctr., *Americans and Text Messaging* 2 (2011), *available at* http://pewinternet.org/~/media//Files/Reports/2011/Americans%20and%20Text%20Messaging.pdf.
[5] *U.S. Wireless Quick Facts*, *supra*.
[6] *Available at* http://judiciary.house.gov/hearings/113th/04252013/Blaze%2004252013.pdf.

than half of Americans,[7] communicate even more frequently with the carrier's network, because they typically check for new email messages every few minutes.[8] When phones communicate with the network, the service provider automatically retains information about such communications, which for calls includes which cell site the phone was connected to at the beginning and end of the call.[9] Most cell sites consist of three directional antennas that divide the cell site into sectors (usually of 120 degrees each).[10] Service providers automatically retain sector information too, which reveals even more precise information about the user's location.[11] In addition to cell site and sector, some carriers also calculate and log the caller's distance from the cell site.[12]

---

[7] Maeve Duggan & Lee Rainie, Pew Research Ctr., *Cell Phone Activities 2012* 12 (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_CellActivities_11.25.pdf.

[8] Gyan Ranjan et al., *Are Call Detail Records Biased for Sampling Human Mobility?*, Mobile Computing & Comm. Rev., July 2012, at 34, *available at* http://www-users.cs.umn.edu/~granjan/Reports/MC2R_2012_CDR_Bias_Mobility.pdf.

[9] Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 Berkeley Tech. L. J. 117, 128 (2012).

[10] Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Attorneys' Bull., Nov. 2011, at 16, 19, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

[11] The availability of historical cell site location information and the length of time it is stored depends on the policies of individual wireless carriers. Sprint/Nextel stores data for 18–24 months; other carriers vary from one year of storage (T-Mobile) to indefinite retention "from July 2008" (AT&T/Cingular). U.S. Dep't of Justice, Retention Periods of Major Cellular Service Providers (Aug. 2010),

The precision of a user's location revealed by the cell site identifier in the carrier's records depends on the size of the sector. The coverage area for a cell site is reduced in areas with greater density of cell towers, with the greatest cell site density and thus smallest coverage areas in urban areas. For example, a searchable database of publicly available information reveals that there are more than 76 towers and 761 antenna sites within a four-mile radius of the Fourth Circuit's courthouse in Richmond.[13]

Cell site density is increasing rapidly, largely as a result of the growth of Internet usage by smartphones. *See* CTIA – The Wireless Association, Semi-Annual Wireless Industry Survey 2 (2012)[14] (showing that the number of cell sites in the United States has more than doubled in the last decade, with 285,561 as of June 2012); *id.* at 8 (wireless data traffic increased by 586% between 2009 and 2012). Each cell site can supply a fixed volume of data required for text messages, emails, web browsing, streaming video, and other uses. Therefore, the only way for providers to maintain adequate coverage as smartphone data usage increases is to

---

available at https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.

[12] *See* Verizon Wireless Law Enforcement Resource Team (LERT) Guide 25 (2009), *available at* http://publicintelligence.net/verizon-wireless-law-enforcement-resource-team-lert-guide/ (providing sample records indicating caller's distance from cell site to within .1 of a mile).

[13] Search conducted using http://www.antennasearch.com.

[14] *Available at* http://files.ctia.org/pdf/CTIA_Survey_MY_2012_Graphics-_final.pdf.

erect more cell sites. As new cell sites are erected, the coverage areas around existing nearby cell sites will be reduced, so that the signals sent by those sites do not interfere with each other. *See* Ctr. for Democracy & Tech., Cell Phone Tracking: Trends in Cell Site Precision 2 (2013).[15]

In addition to erecting new conventional cell sites, providers are also able to increase their network coverage using low-power small cells, called "microcells," "picocells," and "femtocells," which provide service to areas as small as ten meters. *Id.* Femtocells are frequently provided by carriers directly to consumers with poor cell phone coverage in their homes or offices and the number of femtocells nationally now exceeds the number of traditional cell sites. *Id.* at 3. Defendants' wireless carrier, Sprint, was the first carrier to make femtocells available to its customers, in 2007, and had distributed over one million femtocells by October 2012.[16] Because the coverage area of femtocells is so small, callers connecting to a carrier's network via femtocells can be located to a high degree of precision, "sometimes effectively identifying individual floors and rooms within buildings."[17] Blaze Hearing Statement at 12. Femtocells with ranges extending

---

[15] *Available at* https://www.cdt.org/files/file/cell-location-precision.pdf.

[16] Informa Telecoms & Media, *Small Cell Market Status* 4–5 (2013), *available at* http://www.smallcellforum.org/smallcellforum_resources/pdfsend01.php?file=050-SCF_2013Q1-market-status%20report.pdf.

[17] Wireless providers are required by law to be able to identify the location of femtocells, both to comply with emergency calling location requirements (E-911), and to comply with federal radio spectrum license boundaries. *See* 3rd Generation

outside of the building in which they are located can also provide cell connections to passersby, providing highly precise information about location and movement on public streets and sidewalks.[18]

Each call or text message to or from a cell phone generates a location record,[19] and at least some, if not all, of those records will reveal information precise enough to know or infer where a person is at a number of points during the day:

> A mobile user, in the course of his or her daily movements, will periodically move in and out of large and small sectors. Even if the network only records cell tower data, the precision of that data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less precise. For a typical user, over time, some of that data will inevitably reveal locational precision approaching that of GPS.

Blaze Hearing Statement at 15. Importantly, when law enforcement requests historical CSLI, it too cannot know before receiving the records how precise the location information will be. Agents will not have prior knowledge of whether the

---

Partnership Project 2, *Femtocell Systems Overview* 33 (2011), *available at* http://www.3gpp2.org/public_html/specs/S.R0139-0%20v1.0_Femtocell%20Systems%20Overview%20for%20cdma2000%20Wireless%20Communication%20Systems_20110819.pdf.

[18] Tom Simonite, *Qualcomm Proposes a Cell-Phone Network by the People, for the People*, MIT Tech. Rev. (May 2, 2013), *available at* http://www.technologyreview.com/news/514531/qualcomm-proposes-a-cell-phone-network-by-the-people-for-the-people/.

[19] The historical cell records obtained in this case include cell site information for each of Defendants' calls, but not for their text messages. (JA 1974–75.)

surveillance target was in a rural area with sparse cell sites, an urban area with dense cell sites, or a home, doctor's office, or church with femtocells. Likewise, they will not know if a target had a smartphone that communicates with the carrier's network (and thus generates location data) every few minutes, or a traditional feature phone that communicates less frequently.

Knowing periodic information about which cell sites a phone connects to over time can be used to interpolate the path the phone user traveled, thus revealing information beyond just the cell site sector in which the phone was located at discrete points.[20] Law enforcement routinely uses cell site data for this purpose; in this case, the government argued that cell site data points showing Defendants' locations before and after two robberies revealed trajectories that placed them at the businesses in question at relevant times. (JA 2525.) Similar data could just as easily be used to conclude from cell site data points when a person visited their doctor's office or church.

[20] *See, e.g.* Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Syss. Design & Implementation 20 (2011), *available at* https://www.usenix.org/legacy/events/nsdi11/tech/full_papers/Thiagarajan.pdf?CFID=230550685&CFTOKEN=76524860 (describing one algorithm for accurate trajectory interpolation using cell site information).

ii. Defendants' location information obtained by law enforcement reveals voluminous and private information about their locations and movements.

In this case, the government obtained 221 days of cell site location information for each defendant. The records reveal the cell site and sector in which the caller was located when each call began and ended, thus providing law enforcement with a dense array of data about Defendants' locations. (*See, e.g.*, JA 878–85 (sample call records of Defendants from February 4–5, 2011).)[21] Mr. Graham's data include 14,805 separate call records for which CSLI was logged, comprising 29,659 cell site location data points.[22] (JA 2668–3224.) Mr. Jordan's records reveal 14,208 calls for which location information was logged, comprising 28,410 cell site location data points.[23] Mr. Graham and Mr. Jordan respectively

[21] The cell site identifier is found in the last two columns of the spreadsheet. The first digit denotes the sector (2, 3, or 4). The latter three digits are the cell site. Thus, "3038" represents base station 038, sector 3. The "repoll number" represents the switch being used; in the Baltimore area there are two switches used for wireless calls, 400 and 438. (JA 1978.)

[22] The records include information about additional calls and text messages for which cell site location information was not logged, adding up to a total of 20,034 lines of data for Mr. Graham.

[23] Mr. Jordan's records were produced in two sets that were provided to Defendants pursuant to the government's *Brady* disclosure obligations, but were not introduced in full at trial or included in the Joint Appendix. One spreadsheet logs calls made between July 1 and September 18, 2010, using the Sprint/Nextel DirectConnect network. The second spreadsheet logs calls made between September 18, 2010 and February 6, 2011, using Sprint/Nextel's regular cellular network. The two networks use separate antenna arrays, but the records for both types of calls reveal cell site location information.

placed or received an average of 67 and 73.8 calls per day for which location data was recorded and later obtained by the government.[24]

This data is particularly revealing of the defendants' location information because of the density of cell sites in the greater Baltimore area. Sprint/Nextel, the carrier used by both defendants, operates a total of 79 cell sites comprising 231 sector antennas within the Baltimore city limits, and many more cell sites elsewhere in Baltimore County. *See* Exhibits A–B. The company operates a separate network of antennas over which it routes its "DirectConnect" calls, comprising 276 sectors within the city of Baltimore. *See* Exhibits C–D.

The records obtained by the government reveal many details about Defendants' locations and movements during the seven months tracked. For example, Mr. Graham's calls include location records from 167 towers and 369 separate sectors, and over the course of a typical day his records chart his movements between multiple sectors. On November 4, 2010, for example (a randomly selected day), he made and received 69 calls in 36 unique cell site sectors. Even more revealing, during one 38-hour period in October 2010, Mr. Graham made and received 209 calls (an average of 5.5 calls per hour) while located in 55 different cell site sectors. Even records of individual calls provide information about movement: 2,212 of his calls were initiated within one cell site

[24] Mr. Jordan's average call frequency is calculated for the 142-day period when he was using Sprint/Nextel's regular network.

sector and terminated in another, suggesting that he was not stationary during the call. The records thus reveal a granular accounting of Defendants' movements over time.

The records also reveal information about particular locations visited. The most frequently occurring cell site and sector in Mr. Graham's records (switch 400, tower 042, sector 2), is the closest tower and sector to his home. Nearly a third of Mr. Graham's phone calls (4,917) were placed or received while he was located in that sector, providing strong indication of when he was in his home. Of those calls, 77 started in his home sector and ended elsewhere, and 226 started elsewhere and ended when he was at home, providing information about his patterns of movement to and from home as well as his static location there.

The call records reveal other sensitive location information as well. For example, during the period for which records were obtained Mr. Graham's wife was pregnant, and he often accompanied her to appointments with her OB/GYN.[25] Twenty-nine calls during business hours began or ended in the sector where the OB/GYN's office is located,[26] allowing the inference that they were at the doctor's office at those times.

[25] Communications between Meghan Skelton, Counsel for Mr. Graham, and Nathan Freed Wessler, Counsel for Amici.

[26] The nearest tower to the doctor's office is switch 400, tower 177. The office sits on the dividing line between sectors 2 and 4 of that tower, so calls from both sectors are counted.

The records also allow inferences about where Defendants slept, which could reveal private information about the status of relationships and any infidelities.[27] By sorting the data for the first and last calls of each day, one can infer whether a person slept at home or elsewhere. For example, from July 10 to July 15, 2010, Mr. Graham's last call of the night and first call of the morning were either or both placed from his home sector (2042). But on July 9, both the last call of the night and the first call of the next morning were placed from a cell sector 30 minutes from his house (switch 438, tower-sector 4131). This information, like that described above, is deeply sensitive and quintessentially private.

B. Obtaining 221 or 14 Days' Worth of Cell Phone Location Data Is a "Search" Under the Fourth Amendment Requiring a Warrant Based Upon Probable Cause.

The Supreme Court has made clear that when the government engages in prolonged location tracking, or when tracking reveals information about a private space that could not otherwise be observed, that tracking violates a reasonable expectation of privacy and therefore constitutes a search within the meaning of the Fourth Amendment. Acquisition of Defendants' cell phone location information is a search for both of these reasons. Because warrantless searches are "'*per se* unreasonable,'" the acquisition of Defendants' location records violated their

[27] *See* Jane Mayer, *What's the Matter with Metadata?*, New Yorker (June 6, 2013), http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html ("Such data can reveal, too, who is romantically involved with whom, by tracking the locations of cell phones at night.").

Fourth Amendment rights. *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)).

In *United States v. Jones*, five Justices agreed that when the government engages in prolonged location tracking, it conducts a search under the Fourth Amendment. 132 S. Ct. at 964 (Alito, J.); *id.* at 955 (Sotomayor, J.). The case involved law enforcement's installation of a GPS tracking device on a suspect's vehicle and its use to track his location for 28 days. *Id.* at 948. Although the majority opinion relied on a trespass-based rationale to determine that a search had taken place, *id.* at 949, it specified that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* [reasonable-expectation-of-privacy] analysis." *Id.* at 953.

Five Justices conducted a *Katz* analysis, and concluded that longer-term location tracking violates reasonable expectations of privacy. *Id.* at 960, 964 (Alito, J.); *id.* at 955 (Sotomayor, J.). Justice Alito wrote that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 964. This conclusion did not depend on the particular type of tracking technology at issue in *Jones*, and Justice Alito identified the proliferation of mobile devices as "[p]erhaps most significant" of the emerging location tracking technologies. *Id.* at 963. Writing separately, Justice Sotomayor agreed and explained that "GPS monitoring—by making available at a relatively low cost such

a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *Id.* at 956.

The Supreme Court has also made clear that location tracking that reveals otherwise undiscoverable facts about protected spaces implicates the Fourth Amendment. In *United States v. Karo*, 468 U.S. 705 (1984), the Court held that location tracking implicates Fourth Amendment privacy interests because it may reveal information about individuals in areas where they have reasonable expectations of privacy. The Court explained that using an electronic device—there, a beeper—to infer facts about "location[s] not open to visual surveillance," like whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises, was just as unreasonable as searching the location without a warrant. *Id*. at 714–15. Such location tracking, the Court ruled, "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, *id*. at 707, regardless of whether it reveals that information directly or through inference. *See also Kyllo v. United States*, 533 U.S. 27, 36 (2001) (rejecting "the novel proposition that inference insulates a search," noting that it was "blatantly contrary" to the Court's holding in *Karo*

"where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home").

If tracking a car's location for 28 days violates an expectation of privacy that society is prepared to recognize as reasonable, then surely tracking a cell phone's location for 221 days does as well.[28] Just as "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period," *Jones*, 132 S. Ct. at 964 (Alito, J.), so, too, is it society's expectation that government agents would not track the location of a cell phone for 221 days. The expectation that a cell phone will not be tracked is even more acute than is the expectation that cars will not be tracked because individuals are only in their cars for discrete periods of time, but carry their cell phones with them wherever they go, including inside Fourth-Amendment-protected private spaces. Moreover, cars are visible on the public street, whereas individuals generally keep their cell phones in a concealed place when not actively in use. *See United States v. Powell*, __ F. Supp. 2d __, 2013 WL 1876761, at *13 (E.D. Mich. May 3, 2013) ("There are practical limits on where a GPS tracking device attached a person's vehicle may go. A cell phone, on the other hand, is usually carried with a person *wherever* they go.").

Although the district court pointed out that *Jones* addressed real-time

[28] The government's acquisition of 14 days' worth of cell site location information for Defendants' phones pursuant to the initial order also constitutes a search.

location tracking while this case involves historical location data, *United States v. Graham*, 846 F. Supp. 2d 384, 391–92 (D. Md. 2012), that is a distinction without a difference. "The temporal distinction between prospective and historical location tracking is not compelling, because the degree of invasiveness is the same, whether the tracking covers the previous 60 days or the next. . . . 'The picture of [a person's] life the government seeks to obtain is no less intimate simply because it has already been painted.'" *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 839 (S.D. Tex. 2010), *argued*, No. 11–20884 (5th Cir. Oct. 2, 2012). Because there is no meaningful distinction between the information the government seeks in this case and the information the government sought in *Jones*, the government's actions constituted a search.

The district court stated its disagreement with the idea that "traditional surveillance becomes a Fourth Amendment 'search' only after some specified period of time." *Graham*, 846 F. Supp. 2d at 401–02. But this is a straw man, as the concurring opinions in *Jones* are premised on the fact that electronic location monitoring is *not* traditional surveillance, and that it can offend the Fourth Amendment in ways that traditional surveillance typically cannot:

> Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. . . . Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap. . . . [S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single

movement of an individual's car for a very long period.

132 S. Ct. at 963–64 (Alito, J.). The district court erred in discounting the view of five members of the Supreme Court that longer term location tracking obtained by electronic means violates the Fourth Amendment.

Further, cell phone location data implicates Fourth Amendment interests because, like the tracking in *Karo*, it reveals or enables the government to infer information about whether the cell phone is inside a protected location and whether it remains there. The cell phone travels through many such protected locations during the day where, under *Karo*, the government cannot warrantlessly intrude on individuals' reasonable expectations of privacy. *See, e.g. Kyllo*, 533 U.S. at 31 (home); *See v. City of Seattle*, 387 U.S. 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483, 486-88 (1964) (hotel room). "If at any point a tracked cell phone signaled that it was inside a private residence (or other location protected by the Fourth Amendment), the only other way for the government to have obtained that information would be by entry into the protected area, which the government could not do without a warrant." *Powell*, 2013 WL 1876761, at *11.

This is true even if cell phone location data is less precise than GPS data, because even imprecise information, when combined with visual surveillance or a known address can enable law enforcement to infer the exact location of a phone. *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'ns*

Serv. to Disclose Records to the Gov't, 620 F.3d 304, 311 (3d Cir. 2010) ["Third Circuit Opinion"]. Indeed, that is exactly how the government's experts routinely use such data; "the Government has asserted in other cases that a jury should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home." *Id.* at 311–12. In this case, Mr. Graham's cell phone records frequently indicate when he was home. *Supra* Part I.A.ii. Moreover, the rapid proliferation of femtocells means that for many people, cell site location records will reveal their location to the accuracy of a floor or room within their home. When the government requests historical cell site information it has no way to know in advance how many cell site data points will be for femtocells or geographically small sectors of conventional cell towers, or will otherwise reveal information about a Fourth-Amendment-protected location. As the Court observed in *Kyllo*, "[n]o police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." 533 U.S. at 39; *accord Powell*, 2013 WL 1876761, at *12 (applying *Kyllo* to cell site location information). A warrant is therefore required.

Moreover, the government's own use of the records in this case belies its argument that they are imprecise. Although in opposing the motion to suppress the government asserted that CSLI reveals only "general" information about location,

(JA 873–74), at trial the prosecution used Defendants' CSLI to demonstrate when and where Defendants were in the same location together, (JA 2445–46), when Mr. Graham was "right close to the McDonalds," (JA 2524), and the direction and timing of Defendants' movement to and from specific locations, (JA 2525), among other information. Law enforcement combed through seven months of Defendants' location records without a warrant. When the government found 13 location data points that it believed corroborated its theory of the case, it asserted their accuracy and probativeness to the jury. (*See* JA 1983–2009, 2663–66.) But the government incredibly insists that all 58,056 remaining data points reveal nothing private about Defendants' lives. (JA 873–74.) Quite the opposite: long-term data about Defendants' locations and movements reveals much information that society recognizes as justifiably private, and its warrantless acquisition violates the Fourth Amendment.

C. Cell Phone Providers' Ability to Access Customers' Location Data Does Not Eliminate Cell Phone Users' Reasonable Expectation of Privacy in That Data.

The district court concluded that Defendants have no reasonable expectation of privacy in their cell phone location information because, under Supreme Court precedent, that information was "voluntarily" conveyed to Sprint/Nextel and was contained in Sprint/Nextel's business records. *Graham*, 846 F. Supp. 2d at 399. On the contrary, Defendants never voluntarily conveyed their location information to

their wireless carrier, and the Court's business records cases do not extend to the scenario presented here. Moreover, the only circuit to address the issue to date has reached a conclusion directly contrary to the district court's, holding that cell phone users may maintain a reasonable expectation of privacy in their location records even though these records are held by a third party business. *Third Circuit Opinion*, 620 F.3d at 317–18. That is the correct conclusion, and this Court should follow it here.

The district court relied principally on two Supreme Court cases, but neither reaches the government surveillance at issue in this case. In *United States v. Miller*, 425 U.S. 435 (1976), the Court held that a bank depositor had no expectation of privacy in records about his transactions that were held by the bank. Although the Court explained that the records were the bank's business records, *id.* at 440, it proceeded to inquire whether Miller could nonetheless maintain a reasonable expectation of privacy in the records: "We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Id.* at 442. The Court's ultimate conclusion—that Miller had no such expectation—turned not on the fact that the records were owned or possessed by the bank, but on the fact that Miller "voluntarily conveyed" the information contained in them to the bank and its employees. *Id.*

In *Smith v. Maryland*, 442 U.S. 735 (1979), the Court held that the use of a pen register to capture the telephone numbers an individual dials was not a search under the Fourth Amendment. *Id.* at 739, 742. The Court relied heavily on the fact that when dialing a phone number the caller "voluntarily convey[s] numerical information to the telephone company." *Id.* at 744. As in *Miller*, in addition to establishing voluntary conveyance the Court also assessed the degree of invasiveness of the surveillance at issue to determine whether the user had a reasonable expectation of privacy. The Court noted the "pen register's limited capabilities," *id.* at 742, explaining that "'a law enforcement official could not even determine from the use of a pen register whether a communication existed.'" *Id.* at 741 (quoting *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 167 (1977)).

Assessing an individual's expectation of privacy in cell phone location information thus turns on whether the contents of the location records were voluntarily conveyed to the wireless provider, and what privacy interest the person retains in the records. The Third Circuit has explained why cell phone users retain a reasonable expectation of privacy in their location information:

> A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making

> that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."

Third Circuit Opinion, 620 F.3d at 318–19 (last alteration in original).

There is nothing inherent in placing a cell phone call that would indicate to callers that they are exposing their location information to their wireless carrier. In both *Miller* and *Smith*, the relevant documents and dialed numbers were directly and voluntarily conveyed to bank tellers and telephone operators, or their automated equivalents. *See, e.g.*, *Smith*, 442 U.S. at 744. But when a cell phone user makes or receives a call, there is no indication that making or receiving the call will also create a record of the caller's location. The user does not input her location information into the phone, and the phone does not notify the user that her location has been logged. Moreover, unlike the dialed phone numbers at issue in *Smith*, location information does not appear on a typical user's monthly bill. *See id.* at 742. Further, many smartphones include a location privacy setting that, when enabled, prevents applications from accessing the phone's location. However, this setting has no impact at all upon carriers' ability to learn the cell tower in use, thus potentially misleading phone users. Cell-tower location information is automatically determined by the wireless provider, but is not actively, intentionally, or affirmatively disclosed by the caller.

United States v. Bynum, 604 F.3d 161 (4th Cir. 2010), is not to the contrary. In *Bynum*, this Court held that a computer user had no reasonable expectation of

privacy in his internet and phone "'subscriber information'—*i.e.*, his name, email address, telephone number, and physical address" because he had "voluntarily conveyed all this information to his internet and phone companies." *Id.* at 164. The subscriber voluntarily provided this information to the internet and phone companies as part of the process of setting up and registering his accounts. Unlike cell phone location information generated without the user's input or knowledge, he both knew he was conveying that information and intended to do so.

The district court's suggestion that the Sprint/Nextel privacy policy converts automatic, involuntary retention of location information into voluntary conveyance of such data is misplaced. *See Graham*, 846 F. Supp. 2d at 401. The version of the privacy policy in effect when the government requested Defendants' location records devoted a scant four words out of more than 1,500 to noting that some sort of location information is collected. Sprint Nextel Privacy Policy (archived Jan. 11, 2011)[29] ("Information we collect when we provide you with Services includes . . . where it is located . . . ."). The policy did not explain what location information was collected or how long it was retained.[30] Further, the government made no showing that Defendants were actually aware that Sprint's privacy policy existed,

[29] *Available at* http://web.archive.org/web/20110111134604/http://www.sprint.com/legal/privacy.html/.

[30] In fact, the only publicly available information about how long Sprint retains CSLI records comes from documents obtained by the ACLU through public records act requests to municipal police departments. *See supra* note 11.

much less that they read or understood it.[31] *See* (JA 909–10); *see also* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1032 & n.34 (2012) (noting that most consumers do not read privacy policies).

Further, the fact that cell phone location information is handled by a third party is not dispositive. The Sixth Circuit's opinion in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), is instructive. There, the court held that there is a reasonable expectation of privacy in the contents of emails. The court explained that the fact that email is sent through an internet service provider's servers does not vitiate the legitimate interest in email privacy: both letters and phone calls are sent via third parties (the postal service and phone companies), but people retain a reasonable expectation of privacy in those forms of communication. *Id.* at 285 (citing *Katz*, 389 U.S. at 353; *United States v. Jacobsen*, 466 U.S. 109, 114 (1984)). *Warshak* further held that even if a company has a right to access information in certain circumstances under the terms of service (such as to scan

[31] Even if they were aware of its existence, it is likely that Defendants would have thought the privacy policy would *protect against* collection and disclosure of information, not facilitate it. *See* Joseph Turrow et al., *Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace* 1 (2007), *available at* http://www.law.berkeley.edu/files/annenberg_samuelson_advertising.pdf (reporting that most people think the mere existence of a privacy policy on a website means "the site will not share my information with other websites or companies").

emails for viruses or spam), that does not necessarily eliminate the customer's reasonable expectation of privacy vis-à-vis the government. *Id.* at 286–88. In a variety of contexts under the Fourth Amendment, access to a protected area for one limited purpose does not render that area suddenly unprotected from government searches. *See, e.g.*, *United States v. Washington*, 573 F.3d 279, 284 (6th Cir. 2009) (tenants have reasonable expectation of privacy in their apartments even though landlords have a right to enter); *United States v. Stevenson*, 396 F.3d 538, 546 (4th Cir. 2005) ("And the protection of a house extends to apartments, rented rooms within a house, and hotel rooms so that a landlord may not give the police consent to a warrantless search of a rented apartment or room."); *United States v. Paige*, 136 F.3d 1012, 1020 n.11 (5th Cir. 1998) ("[A] homeowner's legitimate and significant privacy expectation . . . cannot be entirely frustrated simply because, *ipso facto*, a private party (*e.g.*, an exterminator, a carpet cleaner, or a roofer) views some of these possessions.").

Like the contents of emails, cell phone location information is not a simple business record voluntarily conveyed by the customer. In this case the government obtained a transcript of two individuals' locations and movements over a staggering 221 days. The Supreme Court has cautioned that new technologies should not be allowed to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34; *see also Warshak*, 631 F.3d at 285 ("[T]he

Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."). If this Court holds that cell phone tracking falls outside of the ambit of the Fourth Amendment, the Supreme Court's decision in *Jones* will have little practical effect in safeguarding Americans from the pervasive monitoring of their movements that so troubled a majority of the Justices. *See Jones*, 132 S. Ct. at 955 (Sotomayor, J.); *id.* at 963–64 (Alito, J.).

II. EVEN IF THE GOOD FAITH EXCEPTION APPLIES, THIS COURT SHOULD DECIDE THE FOURTH AMENDMENT QUESTION.

This Court should decide that a search of long-term historical CSLI requires a probable cause warrant regardless of whether the good faith exception applies. When a case presents a "novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates, there is sufficient reason for the Court to decide the violation issue *before* turning to the good-faith question." *Illinois v. Gates*, 462 U.S. 213, 264, 265 n.18 (1983) (White, J., concurring) (citing *O'Connor v. Donaldson*, 422 U.S. 563 (1975) (finding a constitutional violation and remanding for consideration of the good faith defense)). This is just such a case. Cell site location tracking has become a favored tool of law enforcement and is already used far more frequently than the GPS tracking technology in *Jones*. Its highly intrusive nature cries out for clear judicial regulation. Indeed, the district court explicitly invited clarification about whether

"an aggregation of surveillance records infringes a Fourth Amendment legitimate expectation of privacy." *Graham*, 846 F. Supp. 2d at 394.

In *Warshak*, the Sixth Circuit explained the importance of addressing important Fourth Amendment issues even when the good faith exception will ultimately apply:

> Though we may surely do so, we decline to limit our inquiry to the issue of good faith reliance. If every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the government would be given *carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a statute supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations. In other words, if the exclusionary rule is to have any bite, courts must, from time to time, decide whether statutorily sanctioned conduct oversteps constitutional boundaries.

631 F.3d at 282 n.13 (citation omitted). The Sixth Circuit's logic is not novel: courts frequently decide whether there has been a Fourth Amendment violation before applying the good faith exception. For example, this Court recently decided that warrantless extraction and testing of DNA from a person's clothing violates the Fourth Amendment, and only then applied the good faith exception to the exclusionary rule. *United States v. Davis*, 690 F.3d 226, 247–57 (4th Cir. 2012). Similarly, when assessing whether search warrants satisfy the Fourth Amendment's probable cause and particularity requirements, courts frequently find a Fourth Amendment violation *before* turning to the good faith doctrine. *See, e.g.*, *United States v. Harris*, 215 F. App'x 262, 269–73 (4th Cir. 2007); *United States v.*

Clark, 638 F.3d 89, 91 (2d Cir. 2011); *United States v. Tracey*, 597 F.3d 140, 146–54 (3d Cir. 2010). This approach is no less appropriate in the location tracking context. *See Powell*, 2013 WL 1876761, at *11–20 (holding that government lacked probable cause to engage in cell phone location tracking, and then applying good faith exception); *United States v. Ford*, No. 1:11–CR–42, 2012 WL 5366049, at *7–11 (E.D. Tenn. Oct. 30, 2012) (determining that warrantless GPS tracking violates the Fourth Amendment, and then applying good faith exception).

Phone companies have been inundated with law enforcement requests for location data in recent years: from 2007 and 2012, for example, Sprint/Nextel received nearly 200,000 court orders for cell phone location information. Letter from Vonya B. McCann, Senior Vice President, Sprint, to Rep. Edward J. Markey (May 23, 2012).[32] As the use of cell phones becomes ubiquitous and cell site location information becomes ever-more precise, it is crucial for courts to provide guidance to law enforcement and the public about the scope of the Fourth Amendment. The issue is now before this Court, and addressing it would yield much needed clarity in this Circuit.

[32] *Available at* http://markey.house.gov/sites/markey.house.gov/files/documents/Sprint%20Response%20to%20Rep.%20Markey.pdf.

CONCLUSION

Because the collection of long-term cell phone location information violates reasonable expectations of privacy, this Court should hold that a warrant is required for such searches under the Fourth Amendment.

Respectfully Submitted,

Dated: July 1, 2013

By: /s/ Nathan Freed Wessler
Nathan Freed Wessler
Catherine Crump
Ben Wizner
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500

David R. Rocah
American Civil Liberties Union Foundation of Maryland
3600 Clipper Mill Road,
Suite 350
Baltimore, MD 21211
(410) 889-8555

Kevin S. Bankston
Gregory T. Nojeim
Center for Democracy & Technology
1634 I St NW, Suite 1100
Washington, DC 20006
(202) 637-9800

Hanni Fakhoury
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Thomas K. Maher
Vice-Chair, 4th Circuit
Amicus Committee
National Association of
Criminal Defense Lawyers
123 W. Main St.
Suite 400
Durham, NC 27701
(919) 354-7200

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a) because it contains 6,993 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).
2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman.

/s/ Nathan Freed Wessler

Nathan Freed Wessler

July 1, 2013

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 1st day of July, 2013, the foregoing Amici Curiae Brief for the American Civil Liberties Union Foundation, the American Civil Liberties Union Foundation of Maryland, the Center for Democracy & Technology, the Electronic Frontier Foundation, and the National Association of Criminal Defense Lawyers was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system.

/s/ Nathan Freed Wessler

Nathan Freed Wessler