NO. 12-12928-EE

En Banc Brief

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff/appellee,

v.

QUARTAVIOUS DAVIS,
***Defendant/appellant*.**

On Appeal from the United States District Court
for the Southern District of Florida

EN BANC BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF FLORIDA, INC., AND CENTER FOR DEMOCRACY & TECHNOLOGY IN SUPPORT OF DEFENDANT-APPELLANT

Nancy Abudu
nabudu@aclufl.org
Fla. Bar No. 111881
ACLU Foundation of Florida, Inc.
4500 Biscayne Blvd. Ste. 340
Miami, FL 33137
Tel: 786-363-2700
Fax: 786-363-3108

Nathan Freed Wessler
nwessler@aclu.org
Ben Wizner
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel: 212-549-2500
Fax: 212-549-2654

Benjamin James Stevenson
bstevenson@aclufl.org
Fla. Bar No. 589909
ACLU Foundation of Florida, Inc.
P.O. Box 12723
Pensacola, FL 32591-2723
Tel: 786-363-2738
Fax: 786-363-1985

Gregory T. Nojeim
Harley Geiger
Center for Democracy & Technology
1634 I St NW, Suite 1100
Washington, DC 20006
Tel: 202-637-9800

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

United States v. Quartavious Davis
No. 12-12928

Amici Curiae file this Certificate of Interested Persons and Corporate Disclosure Statement, as required by Local Rules 26.1-1, 28-1(b), and 29-2.

Abudu, Nancy, Counsel for *Amici Curiae*

Agarwal, Amit, United States Attorney's Office

Altman, Roy, United States Attorney's Office

American Civil Liberties Union Foundation, *Amicus Curiae*

American Civil Liberties Union Foundation of Florida, Inc., *Amicus Curiae*

Bankston, Kevin, Former Counsel for Center for Democracy & Technology

Brown, Hon. Stephen T., United States Magistrate Judge

Caruso, Michael, Interim Federal Public Defender

Center for Democracy & Technology, *Amicus Curiae*

Colan, Jonathan, United States Attorney's Office

Crump, Catherine, Former Counsel for *Amici Curiae*

Davis, Quartavious, Defendant/Appellant

Dube, Hon. Robert L., Untied States Magistrate Judge

Electronic Frontier Foundation, *Amicus Curiae*

Fakhoury, Hanni, Counsel for Electronic Frontier Foundation

Ferrer, Wifredo A., United States Attorney's Office

Fisher, Sylvester, Co-Defendant

Garber, Hon. Barry L., United States Magistrate Judge

Geiger, Harley, Counsel for Center for Democracy & Technology

Gold, Hon. Alan S., United States District Judge

Golembe, Stephen J., Co-Defendant Counsel

Hayes, Anne Margaret, Appellate Counsel

Kayanan, Maria, Counsel for *Amici Curiae*

Korchin, Paul M., Assistant Federal Public Defender

Lenard, Hon. Joan A., United States District Judge

Malone, Omar, Co-Defendant Counsel

Markus, David Oscar, Counsel

Martin, Michael, Co-Defendant

Martin, Jahmal A., Co-Defendant

McAliley, Hon. Chris M., United States Magistrate Judge

Michaels, Alexander J., Co-Defendant Counsel

Moss, Jr., Reginald A., Co-Defendant Counsel

National Association of Criminal Defense Lawyers, *Amicus Curiae*

Nojeim, Greg, Counsel for Center for Democracy & Technology

O'Sullivan, Hon. John J., United States Magistrate Judge

Palermo, Hon. Peter R., Untied States Magistrate Judge

Perwin, Amanda, United States Attorney's Office

Quencer, Kevin, United States Attorney's Office

Reid, Jamarquis T., Co-Defendant

Salyer, Kathleen M., United States Attorney's Office

Schultz, Anne R., United States Attorney's Office

Shapiro, Jacqueline E., Appellate Counsel

Sibila, Jorge A., Co-Defendant Counsel

Smith, Willie, Co-Defendant

Stevenson, Benjamin James, Counsel for *Amici Curiae*

Torres, Hon. Edwin G., United States Magistrate Judge

Turnoff, Hon. William C., United States Magistrate Judge

Ungaro, Hon. Ursula, United States District Judge

Wessler, Nathan Freed, Counsel for *Amici Curiae*

White, Hon. Patrick A., United States Magistrate Judge

Wizner, Ben, Counsel for *Amici Curiae*

Williams, Hon. Kathleen M., United States District Judge

Zelman, Michael, Trial Counsel

Corporate Disclosure Statement

Amici Curiae American Civil Liberties Union Foundation, American Civil Liberties Union Foundation of Florida, Inc., and Center for Democracy & Technology are non-profit entities that do not have parent corporations. No publicly held corporation owns 10 percent or more of any stake or stock in *amici curiae*.

/s/ Nathan Freed Wessler

Nathan Freed Wessler

TABLE OF CONTENTS

TABLE OF CITATIONS viii

INTEREST OF AMICI CURIAE 1

STATEMENT OF THE ISSUES 2

SUMMARY OF ARGUMENT 3

ARGUMENT 4

I. THE FOURTH AMENDMENT REQUIRES A WARRANT FOR HISTORICAL CELL SITE LOCATION INFORMATION. 4

A. Cell Site Location Information Reveals Private, Invasive, and Increasingly Precise Information About Individuals' Locations and Movements. 4

B. Obtaining Historical Cell Site Location Information Is a "Search" Under the Fourth Amendment Requiring a Warrant Based Upon Probable Cause. 10

C. Cell Phone Providers' Ability to Access Customers' Location Data Does Not Eliminate Cell Phone Users' Reasonable Expectation of Privacy in That Data. 17

II. IN THIS CASE, WARRANTLESS ACQUISITION OF 67 DAYS' WORTH OF HISTORICAL CELL SITE LOCATION INFORMATION VIOLATED DEFENDANT'S REASONABLE EXPECTATION OF PRIVACY UNDER THE FOURTH AMENDMENT. 23

III. EVEN IF THE GOOD-FAITH EXCEPTION APPLIES, THIS COURT SHOULD DECIDE THE FOURTH AMENDMENT QUESTION. 28

CONCLUSION 30

CERTIFICATE OF COMPLIANCE 32

CERTIFICATE OF SERVICE 33

TABLE OF CITATIONS

Cases

Arizona v. Gant, 556 U.S. 332 (2009) 10

Illinois v. Gates, 462 U.S. 213 (1983) 29

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 (3d Cir. 2010) 15, 17, 19

Katz v. United States, 389 U.S. 347 (1967) 10, 22

Kyllo v. United States, 533 U.S. 27 (2001) 12, 14, 22

O'Connor v. Donaldson, 422 U.S. 563 (1975) 29

Oliver v. United States, 466 U.S. 170 (1984) 24

Riley v. California, 134 S. Ct. 2473 (2014) 13, 23

See v. City of Seattle, 387 U.S. 541 (1967) 14

Smith v. Maryland, 442 U.S. 735 (1979) 18, 19, 20, 21

Stoner v. California, 376 U.S. 483 (1964) 14

Tracey v. State, No. SC11-2254, 2014 WL 5285929 (Fla. Oct. 16, 2014) ..... passim

United States v. Brazel 102 F.3d 1120, (11th Cir. 1997) 22

United States v. Carpenter, No. 12-20218, 2014 WL 943094 (E.D. Mich. Mar. 11, 2014) 28

United States v. Davis, 754 F.3d 1205 (11th Cir. 2014) 13, 15, 19

United States v. Jacobsen, 466 U.S. 109 (1984) 22

United States v. Jones, 132 S. Ct. 945 (2012) ..... passim

United States v. Karo, 468 U.S. 705 (1984) 12, 14

United States v. Madison, No. 11-60285-CR, 2012 WL 3095357 (S.D. Fla. July 30, 2012) 28

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) 3, 13

United States v. Miller, 425 U.S. 435 (1976) 17, 18

United States v. Paige, 136 F.3d 1012 (5th Cir. 1998)..... 22

United States v. Powell, 943 F. Supp. 2d 759 (E.D. Mich. 2013)..... 13

United States v. Washington, 573 F.3d 279 (6th Cir. 2009)..... 22

Constitution and Statutes

18 U.S.C. § 2703..... 2, 10, 13, 17

Other Authorities

3rd Generation Partnership Project 2, *Femtocell Systems Overview* (2011).....8

Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Syss. Design & Implementation (2011).....9

AT&T, *Transparency Report* (2014)..... 30

CTIA – The Wireless Association, *Annual Wireless Industry Survey* (2014).....4

CTIA – The Wireless Association, *Semi-Annual Wireless Industry Survey* (2013).....7

CTIA–The Wireless Association, *U.S. Wireless Quick Facts* (2014).....4

Ctr. for Democracy & Tech., Cell Phone Tracking: Trends in Cell Site Precision (2013)..... 7, 8

Gyan Ranjan et al., *Are Call Detail Records Biased for Sampling Human Mobility?*, Mobile Computing & Comm. Rev. (July 2012).....5

Jane Mayer, *What's the Matter with Metadata?*, New Yorker (June 6, 2013) 26

Letter from Vonya B. McCann, Senior Vice President, Sprint, to Rep. Edward J. Markey (May 23, 2012)..... 30

Maeve Duggan, Pew Research Ctr., *Additional Demographic Analysis* (2013).....5

MetroPCS, MetroPCS Subpoena Compliance, Attach. A to Letter from Steve Cochran, Vice President, MetroPCS Commc'ns, Inc., to Rep. Edward J. Markey (May 23, 2012) 5

Pew Research Ctr., *Mobile Technology Fact Sheet* (2014) 4

Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014) 21

Samia Perkins, *MetroPCS May be the Biggest Winner in AT&T/T-Mobile Deal*, Slash Gear (Mar. 22, 2011) 25

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. (2012) 6

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. (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) 4, 5, 8, 9

Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Attorneys' Bull., (Nov. 2011) 6

Tom Simonite, *Qualcomm Proposes a Cell-Phone Network by the People, for the People*, MIT Tech. Rev. (May 2, 2013) 8

Verizon Wireless, *Law Enforcement Resource Team (LERT) Guide* (2009).....6

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union Foundation ("ACLU") is a nationwide nonpartisan organization of nearly 500,000 members, dedicated to protecting the fundamental liberties and basic civil rights guaranteed by state and federal Constitutions. The ACLU of Florida, a state affiliate of the national ACLU, is devoted to advocacy on behalf of more than 18,000 statewide members and supporters. The ACLU and its affiliates, including the ACLU of Florida, are well-positioned to submit an *amicus* brief in this case. They have long been committed to defending individuals' Fourth Amendment rights and have 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 11th Cir. R. 35-9 this brief is accompanied by a motion for leave to file. Counsel for *amici curiae* certifies that no party objects 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.

STATEMENT OF THE ISSUES

1. Whether the Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B), (d), is unconstitutional under the Fourth Amendment insofar as it authorizes the government to acquire records showing historical cell site location information from a telephone service provider.
2. On the facts of this case, whether the government acquisition, pursuant to an order authorized by the Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B), (d), of cellular telephone records showing historical cell site location information from a telephone service provider constitutes an unreasonable search or seizure in violation of Defendant's constitutional rights under the Fourth Amendment.
3. Whether the Court should address the Fourth Amendment issue regardless of whether it upholds the panel's overbroad application of the good-faith exception to the exclusionary rule.

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 67 days of cell site location information ("CSLI") for 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 67 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 panel correctly held that obtaining and examining CSLI records is a search, and that people do not lose their privacy interest in their sensitive location information merely by signing up for service with a phone company. The Court

should uphold the panel's conclusion that the government's acquisition of Defendant's comprehensive cell phone location information without a warrant violates the Fourth Amendment.

ARGUMENT

I. THE FOURTH AMENDMENT REQUIRES A WARRANT FOR HISTORICAL CELL SITE LOCATION INFORMATION.

A. Cell Site Location Information Reveals Private, Invasive, and Increasingly Precise Information About Individuals' Locations and Movements.

As of December 2013, there were 335.65 million wireless subscriber accounts in the United States, responsible for 2.61 trillion annual minutes of calls and 1.91 trillion annual text messages.[2] Cell phone use has become ubiquitous: more than 90% of American adults own cell phones[3] and more than a third of U.S. households have only wireless telephones.[4]

Cellular telephones regularly communicate with the carrier's network by sending radio signals to nearby base stations, or "cell sites."[5] When turned on,

---

[2] CTIA – The Wireless Association, *Annual Wireless Industry Survey* (2014), *available at* http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

[3] Pew Research Ctr., *Mobile Technology Fact Sheet* (2014), *available at* http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

[4] CTIA–The Wireless Association, *U.S. Wireless Quick Facts* (2014), *available at* http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts.

[5] *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

"[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."[6] 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 than six in ten Americans,[7] communicate even more frequently with the carrier's network, because they typically check for new email messages or other data every few minutes.[8] When phones communicate with the network, the service provider's equipment generates records about that communication, which the provider typically retains.[9] For calls, this data includes

---

(2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) ["Blaze Hearing Statement"], *available at* http://judiciary.house.gov/hearings/113th/04252013/Blaze%2004252013.pdf.

[6] *Id.*

[7] Maeve Duggan, Pew Research Ctr., *Additional Demographic Analysis* (2013), *available at* http://www.pewinternet.org/2013/09/19/additional-demographic-analysis/.

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

[9] The length of time CSLI is stored depends on the policies of individual wireless carriers: AT&T stores data for five years, Sprint/Nextel for 18 months, and MetroPCS for six months. Letter from Timothy P. McKone, Executive Vice President, AT&T, to Rep. Edward J. Markey 3 (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf; Letter from Charles McKee, Vice President, Sprint Nextel, to Hon. Edward J. Markey 2 (Oct. 3, 2013), *available at* http://s3.documentcloud.org/documents/889100/response-sprint.pdf; MetroPCS, MetroPCS Subpoena Compliance, Attach. A to Letter from Steve Cochran, Vice President, MetroPCS Commc'ns, Inc., to Rep. Edward J. Markey (May 23, 2012),

which cell site the phone was connected to at the beginning and end of the call, as well as the "sector" of that cell site.[10] Most cell sites consist of three directional antennas that divide the cell site into sectors (usually of 120 degrees each),[11] but an increasing number of towers have six sectors.[12] In addition to cell site and sector, some carriers also calculate and log the caller's distance from the cell site.[13]

The precision of a user's location revealed by the cell site records depends on the size of the sector. The coverage area for a cell site is smaller in areas with greater density of cell towers, with urban areas having the greatest density and thus the smallest coverage areas. For example, a searchable database of publicly

---

available at http://web.archive.org/web/20130318011325/http://markey.house.gov/sites/markey.house.gov/files/documents/MetroPCS%20Response%20to%20Rep.%20Markey.PDF.

[10] 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).

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

[12] D.E. 283, at 220. Examples of MetroPCS six-sector towers in the Miami area can be found throughout the master list of MetroPCS cell sites. *See, e.g.*, Ex. A, at BS003080–87 (switch Plantation2, towers 3, 7, 10, 13, 20, 111, 119, 201, 202, 206, 207).

[13] *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).

available information reveals that there are 60 towers and 767 antenna sites within a one-mile radius of the Eleventh Circuit's courthouse in Atlanta.[14]

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* (2013)[15] (showing that the number of cell sites in the United States has approximately doubled in the last decade); *id.* (wireless data traffic increased by 9,228% between 2009 and 2013). Each cell site can supply a fixed volume of data required for text messages, emails, web browsing, streaming video, and other uses. Therefore, as smartphone data usage increases, carriers must erect additional cell sites, each covering smaller geographic areas. 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).[16]

In addition to erecting new conventional cell sites, providers are also increasing their network coverage using low-power small cells, called "microcells," "picocells," and "femtocells" (collectively, "femtocells"), which provide service to areas as small as ten meters. *Id.* These devices are often

[14] Search conducted using http://www.antennasearch.com.
[15] *Available at* http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.
[16] *Available at* https://www.cdt.org/files/file/cell-location-precision.pdf.

provided for free to consumers who complain about poor cell phone coverage in their homes or offices. The number of femtocells nationally now exceeds the number of traditional cell sites. *Id.* at 3. 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 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:

---

[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 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 call records obtained in this case include cell site information for each of Defendant's calls, but not for his text messages. *See* D.E. 283, at 229.

> 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 surveillance target was in a rural area with sparse cell sites, an urban area with dense cell sites or six-sector antennas, or a home, doctor's office, or church with femtocells. Likewise, they will not know if a target had a smartphone that communicated with the carrier's network (and thus generated location data) every few minutes, or a traditional feature phone that communicated less frequently. Knowing periodic information about which cell sites a phone connects to over time can also 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

[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?CFI

this case, the government argued that cell site data points showing Defendant's locations leading up one of the robberies revealed a trajectory that placed him at the business in question at the relevant time. D.E. 285, at 37. Similar data could just as easily be used to conclude when a person visited their doctor's office or church.

B. Obtaining Historical Cell Site Location Information 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 cell phone location information is a search for both of these reasons. Because warrantless searches are "'*per se* unreasonable,'" *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)), the acquisition of CSLI pursuant to a Stored Communications Act order on a mere relevance and materiality standard, 18 U.S.C. § 2703(d), violates the Fourth Amendment.

D=230550685&CFTOKEN=76524860 (describing one algorithm for accurate trajectory interpolation using cell site information).

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 at least 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 physically 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").

These precedents provide independent routes to finding that a warrant is required for government investigative access to historical CSLI—and therefore that § 2703(c)(1)(B) and (d) violate the Fourth Amendment when used to obtain CSLI. First, pursuant to the views of five Justices in *Jones*, acquisition of at least longer-term CSLI without a warrant violates the Fourth Amendment. 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.),[21] so, too, is it society's expectation that government agents would not track the location of a cell phone for such a period. 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 to the most private spaces protected by the Fourth Amendment.[22] *United States v. Davis*, 754 F.3d 1205, 1216 (11th Cir. 2014); *United States v. Powell*, 943 F. Supp. 2d 759, 777 (E.D. Mich. 2013).

Although Justice Alito did not define "with precision the point at which"

[21] *See also Maynard*, 615 F.3d at 561–63 ("Prolonged surveillance . . . . [can] reveal more about a person than does any individual trip viewed in isolation. . . . A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car . . . .").

[22] *See Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("[N]early three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.").

tracking becomes "long term," and therefore a search, his reasoning provides guideposts. *Jones*, 132 S. Ct. at 964. Location records covering a period longer than a police officer could reasonably have been expected to have followed a person on foot or by car cross the threshold. *Id.* at 963–64 ("Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."). Most requests for historical CSLI will cover such a period. Historical CSLI therefore enables the government to "monitor and track our cell phones, and thus ourselves, with minimal expenditure of funds and manpower, [which] is just the type of 'gradual and silent encroachment' into the very details of our lives that we as a society must be vigilant to prevent." *Tracey v. State*, No. SC11-2254, 2014 WL 5285929, at *16 (Fla. Oct. 16, 2014).

Moreover, even CSLI records covering a shorter period constitute a search for a second, independent reason. Like the tracking in *Karo*, CSLI reveals or enables the government to infer information about whether the cell phone is inside a protected location and whether it remains there. People carry their cell phones into many such protected locations 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*, 943 F. Supp. 2d at 775. As the panel explained, "the exposure of the cell site location information can convert what would otherwise be a private event into a public one." *Davis*, 754 F.3d at 1216; *see also Riley*, 134 S. Ct. at 2490 ("Historic [cell phone] location information . . . can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

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. Here, the police officer who analyzed Defendant's cell phone location data did just that, testifying at trial that he was able to determine which cell site was nearest to Defendant's home, and to draw

conclusions about when Defendant was and was not at home. D.E. 285, at 42, 49–51. 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. A warrant is therefore required to prevent unauthorized electronic intrusions into the home.

Finally, historical CSLI provides the government with an investigative power it has never had before, a veritable time machine allowing it to reconstruct a person's comings and goings months and years into the past. Irrespective of whether CSLI records reveal a person to have been on public roads or in private spaces, and whether the records cover a short or long time period, police by definition "could not [have] track[ed the suspect] by visual observation," *Tracey*, 2014 WL 5285929, at *19, because they could not have transported themselves back in time to conduct physical surveillance. Therefore, "society's expectation

has been that law enforcement agents and others would not—and indeed, in the main, simply could not" have obtained such a transcript of a person's movements over time and her location in private spaces. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring). Acquisition of historical CSLI is a search, and warrantless requests for it pursuant to § 2703(d) violate 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 government argues that Defendant has no reasonable expectation of privacy in his cell phone location information because that information was conveyed to MetroPCS and was contained in MetroPCS's business records. Brief of United States at 26–29. On the contrary, people do not voluntarily convey their location information to their wireless carriers, and the Court's business records cases do not extend to the scenario presented here. As other appellate courts have explained, users may maintain a reasonable expectation of privacy in their location information even though that information can be determined by a third party business. *Third Circuit Opinion*, 620 F.3d at 317–18; *Tracey*, 2014 WL 5285929, at *16. That is the correct conclusion, and this Court should follow it here.

The Supreme Court cases on which the government relies do not reach the 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 short-term 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 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 (citation omitted).

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); *accord Davis*, 754 F.3d at 1216–17.

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. Unlike the information at issue in those cases, people do not input or knowingly transmit their location information to their wireless carrier. When a cell phone user makes or receives a call, there is no indication that making or receiving the call will cause a record of

the caller's location to be created and retained. 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 sector in use, thus giving phone users a false sense of privacy. Cell site location information is automatically determined by the wireless provider, but is not actively, intentionally, or affirmatively disclosed by the caller.

The government acknowledged as much at trial. During the prosecution's case in chief, MetroPCS's custodian of records testified that "the caller and receiver, they never know what is going on" when calls are routed between cell towers. D.E. 283, at 223. At the start of its closing argument, the prosecution explained that "what this defendant could not have known was that . . . his cell phone was tracking his every moment." D.E. 287, at 4–5. And later in the prosecution's closing, counsel for the government stated that Defendant and his alleged co-conspirators "had no idea that by bringing their cell phones with them to these robberies they were allowing MetroPCS . . . to follow their movements." *Id.* at 14.

Even if *some* people are now aware that service providers log CSLI because of news coverage about the government's requests for that data, the reasonable

expectation of privacy in the information is not diminished. "[T]he Supreme Court [has] cautioned that where an individual's subjective expectations have been 'conditioned' by influences alien to the well-recognized Fourth Amendment freedoms, a normative inquiry may be necessary to align the individual's expectations with the protections guaranteed in the Fourth Amendment." *Tracey*, 2014 WL 5285929, at *19 (citing *Smith*, 442 U.S. at 740 n.5). The inexorable outcome of this normative analysis is that people retain a reasonable expectation of privacy in their CSLI. Indeed, the depth of that expectation is illustrated by recent polling data showing that people consider their cell phone location information to be highly private—more sensitive even than the contents of their text messages, a list of numbers they have called or websites they have visited, or their relationship history.[23]

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

[23] Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 32, 34 (Nov. 12, 2014) *available at* http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

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 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. 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."); *United States v. Brazel*, 102 F.3d 1120, 1148 (11th Cir. 1997) ("[A] landlord generally lacks common authority to consent to a search of a tenant's apartment . . . ."). The sensitive and private information disclosed by CSLI deserves no less protection.

Like the contents of emails, cell phone location information is not a simple business record voluntarily conveyed by the customer. 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.). As the Florida Supreme Court recently explained, "'[t]he fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by "choosing" to carry a cell phone must be rejected.'" *Tracey*, 2014 WL 5285929, at *17.

II. IN THIS CASE, WARRANTLESS ACQUISITION OF 67 DAYS' WORTH OF HISTORICAL CELL SITE LOCATION INFORMATION VIOLATED DEFENDANT'S REASONABLE EXPECTATION OF PRIVACY UNDER THE FOURTH AMENDMENT.

A categorical ruling that the Fourth Amendment requires law enforcement to obtain a warrant before requesting historical CSLI is the better way to resolve this case. As the Supreme Court recently opined, "[i]f police are to have workable rules, the balancing of the competing interests . . . 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'" *Riley*, 134 S. Ct. at 2491–92 (some internal quotation marks omitted; second alteration in original); *accord Oliver v. United States*, 466 U.S. 170, 181

(1984); *Tracey*, 2014 WL 5285929, at *14. A ruling in this case should account for the ever-increasing precision of CSLI and the increasing invasiveness of historical CSLI records, *see supra* Part I.A, and should provide the government and the public with a bright-line rule requiring a warrant for CSLI. Nonetheless, analysis of the actual records obtained by the government without a warrant in this case demonstrates that the government violated Defendant's reasonable expectation of privacy.

The government obtained 67 days of cell site location information for Defendant and his alleged co-conspirators. 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 these men's locations. *See* Ex. B;[24] Gov't Trial Exs. 32–35 (call detail records for Jamarquis Reid, Willie Smith, Jahmal Martin, and Quartavious Davis).[25] Defendant's data include 5,803 separate call records for which CSLI was logged, comprising 11,606 cell site location data points. Ex. B. Mr. Smith's and Mr. Martin's records reveal 5,676 and 3,668 calls for which location information was logged, respectively. Gov't Trial Exs. 33 & 34. Defendant placed or received an average of 86 calls per day for

[24] Cited exhibits were submitted with *Amici*'s panel brief.

[25] The sixth-to-last column of the spreadsheets provides the routing switch for the cell site. The next two columns provide the sector and cell site the phone connected to at the start of the call; the last two columns provide the same information for the end of the call. D.E. 283, at 210–12, 224–25

which location data was recorded and later obtained by the government. Accounting for location information collected at the start and end of each call, this amounts to an average of *one location point every eight minutes*.

This data is particularly revealing of location information because of the density of cell sites in the greater Miami area. MetroPCS, the carrier used by Defendant, operated a total of 214 cell sites comprising 714 sector antennas within Miami-Dade County, and many more cell sites elsewhere in southern Florida, at the time Defendant's location records were obtained. *See* Ex. A. These figures may actually underrepresent the density of cell sites available to MetroPCS customers in southern Florida because the company had roaming agreements with other carriers, significantly expanding its coverage and the number of cell towers its users' phones could connect to.[26]

The records obtained by the government reveal many details about Defendant's locations and movements during the two months tracked. For example, Defendant's calls include location records from 55 towers and 113 separate sectors, and over the course of a typical day his records chart his movements between multiple sectors. On August 13, 2010, for example, he made

[26] *See* Samia Perkins, *MetroPCS May be the Biggest Winner in AT&T/T-Mobile Deal*, Slash Gear (Mar. 22, 2011), http://www.slashgear.com/metropcs-may-be-the-biggest-winner-in-attt-mobile-deal-22141766/ ("[MetroPCS] ha[s] been adept at securing roaming agreements to use competitor's networks . . . ."); D.E. 283, at 234.

and received 108 calls in 22 unique cell site sectors. Even records of individual calls provide information about movement: 378 of his calls were initiated within one cell site sector and terminated in another, suggesting that he was not stationary during the call. The records thus reveal a granular accounting of Defendant's movements over time.

The records also reveal information about particular locations visited. The most frequently occurring cell site and sector in Defendant's records (switch Plantation1, tower 129, sector 2), corresponds to his residence at that time. From August 1–20, 2010, the call records logged Defendant's location in that sector 2,134 times, providing strong indication of when he was in his home. Over the whole 67-day period, 37 calls started in his home sector and ended elsewhere, and 131 calls started elsewhere and ended when he was in or near home, providing information about his patterns of movement to and from home as well as his static location there.

The records also allow inferences about where Defendant 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

[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.").

person slept at home or elsewhere.[28] For example, from August 2 to August 31, 2010, Defendant's last call of the night and first call of the morning were either or both placed from his home sector (2-129). But on September 1 and 2, 2010, both the last call of the night and the first call of the next morning were placed from a location in a neighboring community (sector 2 of cell site 400, switch Plantation2). This information, like that described above, is deeply sensitive and quintessentially private.

Moreover, the government's own use of the records in this case belies its argument that they are imprecise and therefore constitutionally unprotected. Although in opposing the motion to suppress the government asserted that CSLI is "not precise," D.E. 277, at 13, at trial the prosecution used Defendant's CSLI to demonstrate, among other things, that Defendant was "literally right up against the Amerika Gas Station immediately preceding and after that robbery occurred," D.E. 285, at 58, that he was "literally . . . right next door to the Walgreen's just before and just after that store was robbed," *id.* at 61, and that Defendant and his alleged co-conspirators were "literally right on top of the Advance Auto Parts one minute before that robbery took place, D.E. 287, at 13. The government relied on Defendant's CSLI to show where he was, who he was with, and what he was doing. *See* Ex. C; D.E. 285, at 23–38, 55–56, 58, 61, 64–65, 66; D.E. 287, at 4–5,

[28] The government actually conducted such an analysis in this case. D.E. 285, at 48–52.

12–15, 23, 63–66. Law enforcement combed through two months of Defendant's location records without a warrant. When the government found 39 of Defendant's location data points that it believed corroborated its theory of the case, Ex. C, it asserted their accuracy and probativeness to the jury. *See, e.g.*, D.E. 285, at 23–35.[29] But the government incredibly insists that all 11,567 remaining data points reveal nothing private about Defendant's life. D.E. 277, at 13, 35. Quite the opposite: long-term data about Defendant's locations and movements reveals much information that society recognizes as justifiably private, and its warrantless acquisition violates the Fourth Amendment. The panel was correct that obtaining Defendant's historical CSLI was a Fourth Amendment search.

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

The panel was right to decide that a search of historical CSLI requires a probable cause warrant *before* addressing whether the good-faith exception to the

[29] This case is certainly no anomaly in that regard. *See, e.g.*, Excerpt Transcript of Trial Proceedings at 37, *United States v. Madison*, No. 11-60285-CR, 2012 WL 3095357 (S.D. Fla. July 30, 2012), ECF No. 396 (Government's closing argument) ("The Brink's truck gets to the bank on 9/10 at approximately -- between 12:04 and 12:15. And lo and behold, what do we see? . . . The cellphone records says that Brown is there."), *appeal stayed pending decision in Davis*, No. 13-14541 (11th Cir. Oct. 21, 2014); Jury Trial Transcript – Vol. Eight at 55–56, *United States v. Carpenter*, No. 12-20218, 2014 WL 943094 (E.D. Mich. Mar. 11, 2014), ECF No. 333 (Government closing argument) ("Little Tim's phone just happened to be right where the first robbery was at the exact time of the robbery, the exact sector."), *appeal filed*, No. 14-1572 (6th Cir.).

exclusionary rule applies. The en banc Court should do the same, whether or not it leaves in place the panel's overbroad application of the good-faith exception.

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)). 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.

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).

This course is particularly important given the pervasive use of historical cell phone location records by police. Phone companies have been inundated with law enforcement requests for location data in recent years: from 2007 to 2012, for example, Sprint/Nextel received nearly 200,000 court orders for cell phone location information.[30] Similarly, AT&T received 30,886 requests for cell phone location information in just the first six months of 2014.[31] As the use of cell phones becomes near-universal 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.

CONCLUSION

Because the collection of 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.

---

[30] Letter from Vonya B. McCann, Senior Vice President, Sprint, to Rep. Edward J. Markey (May 23, 2012), a*vailable at* http://web.archive.org/web/20130415200646/http://markey.house.gov/sites/markey.house.gov/files/documents/Sprint%20Response%20to%20Rep.%20Markey.pdf.

[31] AT&T, *Transparency Report*, 4 (2014), *available at* http://about.att.com/content/dam/csr/PDFs/ATT_Transparency%20Report_July%202014.pdf.

Respectfully Submitted,

Dated: November 14, 2014

By: /s/ Nathan Freed Wessler
Nathan Freed Wessler
nwessler@aclu.org
Ben Wizner
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel: 212-549-2500
Fax: 212-549-2654

Nancy Abudu
nabudu@aclufl.org
Fla. Bar No. 111881
ACLU Foundation of Florida, Inc.
4500 Biscayne Blvd. Ste. 340
Miami, FL 33137
Tel: 786-363-2700
Fax: 786-363-3108

Benjamin James Stevenson
bstevenson@aclufl.org
Fla. Bar No. 589909
ACLU Foundation of Florida, Inc.
P.O. Box 12723
Pensacola, FL 32591-2723
Tel: 786-363-2738
Fax: 786-363-1985

Gregory T. Nojeim
Harley Geiger
Center for Democracy & Technology
1634 I St NW, Suite 1100
Washington, DC 20006
Tel: 202-637-9800

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a) because it contains 6,999 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

November 14, 2014

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 14th day of November, 2014, the foregoing Amici Curiae Brief for the American Civil Liberties Union Foundation, American Civil Liberties Union Foundation of Florida, and Center for Democracy & Technology 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