

NOS. 14-1572 & 14-1805

IN THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

TIMOTHY IVORY CARPENTER
and
TIMOTHY SANDERS,
Defendants-Appellants.

On Appeal from the United States District Court
for the Eastern District of Michigan, Southern Division

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

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

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
American Civil Liberties Union Fund
of Michigan
2966 Woodward Ave.
Detroit, MI 48201
(313) 578-6800

Rachel Levinson-Waldman
Michael W. Price
Brennan Center for Justice at NYU
School of Law
161 Avenue of the Americas,
12th Floor
New York, NY 10013
(646) 292-8335
rachel.levinson.waldman@nyu.edu
michael.price@nyu.edu

Hanni Fakhoury
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
hanni@eff.org

Gregory T. Nojeim
Center for Democracy and Technology
1634 Eye St., NW
Suite 1100
Washington, DC 20006
(202) 637-9800

Kristina W. Supler, Esq.
Vice Chair, 6th Circuit, Amicus Committee
National Association of Criminal
Defense Lawyers
McCarthy, Lebit, Crystal & Liffman Co.,
L.P.A.
101 Prospect, W., Suite 1800
Cleveland, Ohio 44115-1088
Phone: (216) 696-1422, Ext. 273
Facsimile: (216) 696-1210
kws@mccarthylebit.com

CORPORATE DISCLOSURE STATEMENT

Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Michigan, Brennan Center for Justice, Center for Democracy & Technology, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers 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

CORPORATE DISCLOSURE STATEMENT	i
TABLE OF CONTENTS.....	ii
TABLE OF AUTHORITIES	iii
INTEREST OF AMICI CURIAE.....	vi
STATEMENT REGARDING ORAL ARGUMENT.....	x
SUMMARY OF ARGUMENT	1
ARGUMENT.....	2
I. WARRANTLESS ACQUISITION OF LONG-TERM HISTORICAL CELL SITE LOCATION INFORMATION VIOLATED DEFENDANTS’ REASONABLE EXPECTATION OF PRIVACY UNDER THE FOURTH AMENDMENT.....	2
A. Defendants’ CSLI Obtained by the Government Reveals Invasive and Accurate Information About Their Location and Movements Over Time.	2
i. CSLI reveals private, invasive, and increasingly precise information about individuals’ locations and movements.....	2
ii. Defendants’ location information obtained by law enforcement reveals voluminous and private information about their locations and movements.	9
B. Obtaining 127 or 88 Days’ Worth of Cell Phone Location Data Is a “Search” Under the Fourth Amendment Requiring a Warrant Based Upon Probable Cause.	12
C. Cell Phone Providers’ Ability to Access Customers’ Location Data Does Not Eliminate Cell Phone Users’ Reasonable Expectation of Privacy in That Data.	21
II. EVEN IF THE GOOD FAITH EXCEPTION APPLIES, THIS COURT SHOULD DECIDE THE FOURTH AMENDMENT QUESTION.	27
CONCLUSION.....	29
CERTIFICATE OF COMPLIANCE.....	32
CERTIFICATE OF SERVICE	33
DESIGNATION OF RELEVANT DISTRICT COURT DOCUMENTS.....	34

TABLE OF AUTHORITIES

Cases

<i>Amnesty Int’l USA v. Clapper</i> , 638 F.3d 118 (2d Cir. 2011).....	vi
<i>Arizona v. Gant</i> , 556 U.S. 332 (2009)	12
<i>Commonwealth v. Augustine</i> , 4 N.E. 3d 846	21
<i>Commonwealth v. Augustine</i> , 4 N.E. 3d 846, 863 (Mass. 2014)	21
<i>Commonwealth v. Augustine</i> , 4 N.E.3d 846 (Mass. 2014)	vii
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001)	22
<i>Florida v. Jardines</i> , 133 S. Ct. 1409 (2013)	22
<i>Hepting v. AT&T Corp.</i> , 539 F.3d 1157 (9th Cir. 2008).....	vi
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983)	28
<i>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</i> , 620 F.3d 304 (3d Cir. 2010).....	vii, 17, 21, 24
<i>In re Application of U.S. for Historical Cell Site Data</i> , 724 F.3d 600 (5th Cir. 2013).....	vii
<i>In re Nat’l Sec. Agency Telecomms. Records Litigation</i> , 564 F. Supp. 2d 1109 (N.D. Cal. 2008)vi	
<i>In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.</i> , 15 F. Supp. 3d 466 (S.D.N.Y. 2014), <i>appeal docketed</i> , No. 14-2985 (2d Cir. Aug. 12, 2014). vi	
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	13, 26
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	14, 16, 22, 27
<i>O’Connor v. Donaldson</i> , 422 U.S. 563 (1975).....	28
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	vi, vii, 15, 16
<i>See v. City of Seattle</i> , 387 U.S. 541 (1967).....	16
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	passim
<i>State v. Earls</i> , 70 A.3d 63 (N.J. 2013)	21
<i>Stoner v. California</i> , 376 U.S. 483 (1964).....	16
<i>Tracey v. State</i> , 152 So. 3d 504 (Fla. 2014).....	16, 21, 25, 27
<i>United States v. Cooper</i> , No. 13-cr-00693-SI-1, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015).....	21
<i>United States v. Davis</i> , 754 F.3d 1205 (11th Cir. 2014), <i>rehearing en banc granted</i> 573 F. App’x 925 (mem.).....	vii, 17, 21
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984).....	26
<i>United States v. Jones</i> , 132 S. Ct. 945 (2012).....	passim
<i>United States v. Karo</i> , 468 U.S. 705 (1984)	14, 15, 16
<i>United States v. Maynard</i> , 615 F.3d 544 (D.C. Cir. 2010), <i>aff’d sub nom. United States v. Jones</i> , 132 S. Ct. 945 (2012).....	1
<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	2, 22, 23
<i>United States v. Powell</i> , 943 F. Supp. 2d 759 (E.D. Mich. 2013)	16
<i>United States v. Skinner</i> , 690 F.3d 772 (6th Cir. 2012).....	1, 19, 20
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)	26, 27, 28
<i>United States v. Washington</i> , 573 F.3d 279 (6th Cir. 2009)	26

Statutes

18 U.S.C. § 2703(d) 9, 13

Other Authorities

3rd Generation Partnership Project 2, *Femtocell Systems Overview* (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.....7

Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Syss. Design & Implementation (2011) , available at https://www.usenix.org/legacy/events/nsdi11/tech/full_papers/Thiagarajan.pdf?CFID=230550685&CFTOKEN=76524860.....8

AT&T, *Transparency Report* (2015), available at http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_January_2015.pdf..... 29

CTIA – The Wireless Association, *Annual Wireless Industry Survey* (2014)..... 3

Ctr. for Democracy & Tech., *Cell Phone Tracking: Trends in Cell Site Precision* (2013), available at <https://www.cdt.org/files/file/cell-location-precision.pdf>..... 6

Gyan Ranjan et al., *Are Call Detail Records Biased for Sampling Human Mobility?*, *Mobile Computing & Comm. Rev.* (July 2012), available at http://www-users.cs.umn.edu/~granjan/Reports/MC2R_2012_CDR_Bias_Mobility.pdf..... 4

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> 12

Letter from Charles McKee, Vice President, Sprint Nextel, to Hon. Edward J. Markey (Oct. 3, 2013), available at <http://s3.documentcloud.org/documents/889100/response-sprint.pdf>..... 4

Letter from Timothy P. McKone, Executive Vice President, AT&T, to Rep. Edward J. Markey (Oct. 3, 2013), available at http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf 4

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), available at <http://web.archive.org/web/20130318011325/http://markey.house.gov/sites/markey.house.gov/files/documents/MetroPCS%20Response%20to%20Rep.%20Markey.PDF> 4

Pew Research Ctr., *Mobile Technology Fact Sheet* (2014) 3, 4

Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014), available at http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf. 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. 117 (2012) 4

Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January–June 2014*, available at <http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201412.pdf> . 3

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) 3, 4, 6, 7

Thomas A. O’Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Attorneys’ Bull., 16 (Nov. 2011) available at http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf..... 5

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/> 7

Verizon Wireless, *Law Enforcement Resource Team (LERT) Guide* (2009), available at <http://publicintelligence.net/verizon-wireless-law-enforcement-resource-team-lert-guide/> 5

INTEREST OF AMICI CURIAE¹

The American Civil Liberties Union (“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 of Michigan is a state affiliate of the national ACLU. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to both organizations. The ACLU and ACLU of Michigan have been at the forefront of numerous state and federal cases addressing the right of privacy.

The Brennan Center for Justice at NYU School of Law² is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice, including access to the courts and constitutional limits on the government’s exercise of power. The Center’s Liberty and National Security (LNS) Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic counterterrorism policies, including the dragnet collection of Americans’

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.

² This brief does not purport to represent the position of NYU School of Law.

communications and personal data, and the concomitant effects on privacy and First Amendment freedoms. As part of this effort, the Center has filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014), *appeal docketed*, No. 14-2985 (2d Cir. Aug. 12, 2014); *Amnesty Int’l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011); *Hepting v. AT&T Corp.*, 539 F.3d 1157 (9th Cir. 2008); and *In re Nat’l Sec. Agency Telecomms. Records Litigation*, 564 F. Supp. 2d 1109 (N.D. Cal. 2008).

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.

EFF is a member-supported civil liberties organization based in San Francisco, California and works to protect innovation, free speech, and privacy in the digital world. With over 25,000 active donors and dues-paying members nationwide, EFF represents the interests of technology users in both court cases

and in broader policy debates surrounding the application of law in the digital age. As part of its mission, EFF has served as amicus curiae in landmark state and federal cases addressing Fourth Amendment issues raised by emerging technologies, including location-based tracking technologies like GPS and cell-site tracking. *See, e.g., Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014), *rehearing en banc granted* 573 F. App'x 925 (mem.); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *In re Application of U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014).

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.

STATEMENT REGARDING ORAL ARGUMENT

Amici curiae submit that oral argument is appropriate in this case because the Fourth Amendment question on appeal is an issue of significant importance and has not yet been resolved in this Circuit. *Amici curiae* respectfully seek leave to participate in oral argument on the Fourth Amendment question, because their participation may be helpful to the Court in addressing the novel and important issues presented by this appeal. *See* 6 Cir. R. 29.

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 more than four months of cell site location information (“CSLI”) without a warrant. If tracking a vehicle for 28 days in *Jones* was a search, then surely tracking a cell phone for four times as long 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 relied on this Court’s opinion in *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), but the district court’s reasoning rests on an

unjustifiably expansive reading of that case, which involved less than three days of tracking revealing only a suspect's movements on public roadways during a single multistate car trip. Nor does Supreme Court jurisprudence regarding bank records and dialed telephone numbers, *see Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976), govern the outcome of this case, 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' CSLI Obtained by the Government Reveals Invasive and Accurate Information About Their Location and Movements Over Time.

- i. CSLI 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 2.62 trillion annual minutes of calls

and 1.91 trillion annual text messages.³ Cell phone use has become ubiquitous: more than 90% of American adults own cell phones⁴ and 44% of U.S. households have only wireless telephones.⁵

Cellular telephones regularly communicate with the carrier's network by sending radio signals to nearby base stations, or "cell sites."⁶ 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."⁷ When phones send or receive calls or text messages, the service provider's equipment generates records about that communication, which the

³ CTIA – The Wireless Ass'n, *Annual Wireless Industry Survey* (2014), available at <http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey>.

⁴ Pew Research Ctr., *Mobile Technology Fact Sheet* (2014), available at <http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/>.

⁵ Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January–June 2014* 1, available at <http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201412.pdf>.

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. 6 (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>.

⁷ *Id.*

provider typically retains.⁸ Smartphones, which are now used by almost six in ten Americans,⁹ communicate even more frequently with the carrier's network, because they typically check for new email messages or other data every few minutes.¹⁰ For calls (and increasingly for text messages and data connections), the data stored by service providers includes 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.¹¹ Most cell sites consist of three directional antennas that divide the cell site into

⁸ 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), *available at* <http://web.archive.org/web/20130318011325/http://markey.house.gov/sites/markey.house.gov/files/documents/MetroPCS%20Response%20to%20Rep.%20Markey.PDF>.

⁹ Pew Research Ctr., *supra*.

¹⁰ 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.

¹¹ 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).

sectors (usually of 120 degrees each),¹² but an increasing number of towers have six sectors.¹³ In addition to cell site and sector, some carriers also calculate and log the caller's distance from the cell site.¹⁴

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. *See* Ex. B.

Cell site density is increasing rapidly, largely as a result of the growth of internet usage by smartphones. *See* CTIA, *Annual Wireless Industry Survey*, *supra* note 3 (showing that the number of cell sites in the United States nearly doubled from 2003 to 2013); *id.* (wireless data usage 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

¹² 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.

¹³ (R332, Tr. 12/13/13, Page ID 3023). Examples of MetroPCS six-sector towers in the Detroit area can be found throughout the master list of MetroPCS cell sites. *See* Ex. A.

¹⁴ *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).

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.¹⁵ Carriers also accommodate growing network usage by erecting six-sector cell sites, which result in smaller sectors and therefore “more precise” location information. (R332, Tr. 12/13/13, Page ID 3023).

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.¹⁶ These devices are often 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.¹⁷ 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.”¹⁸ Femtocells with ranges extending outside of the building in which

¹⁵ See Ctr. for Democracy & Tech., Cell Phone Tracking: Trends in Cell Site Precision 2 (2013), available at <https://www.cdt.org/files/file/cell-location-precision.pdf>.

¹⁶ *Id.* at 2.

¹⁷ *Id.* at 3.

¹⁸ Blaze Hearing Statement, *supra*, at 12. Wireless providers are required 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

they are located can also provide cell connections to passersby, providing highly precise information about location and movement on public streets and sidewalks.¹⁹

Each call or text message to or from a cell phone generates a location record,²⁰ 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.²¹

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.

¹⁹ 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/>.

²⁰ The records obtained in this case include cell site information for Defendants' calls, but not for their text messages.

²¹ Blaze Hearing Statement, *supra*, 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 communicates with the carrier's network (and thus generates location data) every few minutes, or a traditional feature phone that may communicate 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 where the phone was located at discrete points.²² Law enforcement routinely uses cell site data for this purpose; in this case, the government presented testimony explaining that cell site data points revealed Mr. Carpenter's trajectories placing him at the businesses in question at the relevant times. (*See* R332, Tr. 12/13/13, Page ID 3017, 3019, 3024). Similar data could just as easily be used to conclude when a person visited their doctor's office or church.

²² *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, using orders issued under 18 U.S.C. § 2703(d), the government requested from Defendants' service providers more than five months of historical cell site location information for Mr. Carpenter, (R221-3, Appl. & Order, Page ID 1153–1161; R221-4, Appl. & Order, Page ID 1164–1172), and more than six months of historical CSLI for Mr. Sanders, (R221-2, Appl. & Order, Page ID 1141–1150). The government actually obtained 127 days of CSLI for Mr. Carpenter and 88 days of records for Mr. Sanders.²³ *See* Exs. D & E. The records reveal the cell site and sector in which each defendant was located when calls began and ended, thus providing law enforcement with a dense array of data about Defendants' locations. *See, e.g.*, Ex. C, Def. Trial Ex. 3 (sample of records).²⁴ Mr. Carpenter's data include 6,449 separate call records for which CSLI was logged, comprising 12,898 cell site location data points.²⁵ Ex. D. Mr. Sanders's records reveal 11,517 calls for which location information was logged, comprising 23,034 cell site location data points. Ex. E. Mr. Carpenter and Mr. Sanders respectively

²³ Copies of the CSLI records obtained by the government were turned over to the defense in discovery, and then provided to *amici curiae* during preparation of this brief. *Amici* are filing them as attachments.

²⁴ The cell site and sector information in Mr. Carpenter's records is found in the last five columns of the spreadsheet. (R332, Tr. 12/13/13, Page ID 3031–3032).

²⁵ The records include information about additional calls for which CSLI was not logged, adding up to a total of 7,958 lines of data for Mr. Carpenter.

placed or received an average of 50.8 and 130.9 calls per day for which location data was recorded and later obtained by the government. For Mr. Sanders, that amounts to an average of 261 location points per day, or one location point every six minutes.

This data is particularly revealing of Defendants' location information because of the density of cell sites in the greater Detroit area. MetroPCS, the carrier used by Mr. Carpenter, operates a total of 260 cell sites comprising 1035 sector antennas within Wayne County, Michigan, and many more cell sites elsewhere in southeastern Michigan. *See* Exs. A, B.

The records obtained by the government reveal many details about Defendants' locations and movements. For example, Mr. Carpenter's calls show his location in more than 200 separate sectors, and over the course of a typical day his records chart his movements between multiple sectors. On one day, March 19, 2011, he made and received 141 calls while located in 40 unique cell site sectors. Even records of individual calls provide information about movement: from March 17 to March 31, 2011, for example, 374 of his calls were initiated within one cell site sector and terminated in another, suggesting that he was not stationary during the calls. The records thus reveal a granular accounting of Defendants' movements over time.

The records also reveal information about particular locations visited. The cell site and sector closest to Mr. Carpenter's home is sector 3 of tower 465, switch Detroit1. During one two-week period (March 17–31, 2011), 117 of Mr. Carpenter's phone calls were placed or received while he was located in that sector, providing strong indication of when he was in his home. Of those calls, 11 started in his home sector and ended elsewhere, and seven started elsewhere and ended when he was at or near 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, Mr. Carpenter attended a church in Detroit during the period for which records were obtained.²⁶ In the early afternoon on a number of Sundays, Mr. Carpenter made or received calls from the overlapping sectors in which the church is located (tower 109, sector 2 and tower 476, sector 2). *See, e.g.*, Ex. D at 94/158 (February 20, 2011); *id.* at 107/171 (February 27, 2011); *id.* at 123/187 (March 6, 2011); *id.* at 149/213 (March 20, 2011). Those cell site sectors do not routinely appear in Mr. Carpenter's records on other days of the week, leading to the inference that he was worshipping at those times.

The records also allow inferences about where Defendants slept, which could reveal private information about the status of relationships and any

²⁶ Telephone communication between Nathan Freed Wessler, Counsel for *Amici*, and Timothy Carpenter, Defendant.

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, on the nights of December 23–27, 2010, Mr. Carpenter’s last call of the night and/or first call of the morning were from the sector nearest his home (465-3). *See* Ex. D at 66, 71, 73, 75, 77. But on the night of December 22, 2010, the last call of the night and first call of the next morning were placed from overlapping sectors in a Detroit neighborhood approximately four miles from his home (tower 401, sector 5 and tower 445, sector 1). This information, like that described above, is deeply sensitive and quintessentially private.

B. Obtaining 127 or 88 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 location tracking by law enforcement violates a reasonable expectation of privacy, and therefore constitutes a search within the meaning of the Fourth Amendment, when such tracking is either a) prolonged, or b) reveals information about a private space that could not otherwise be observed. 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*

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.”).

States, 389 U.S. 347, 357 (1967)), the acquisition of Defendants' location records using an order issued on a mere relevance and materiality standard, *see* 18 U.S.C. § 2703(d), violated their Fourth Amendment rights.

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 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,” *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. 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.),²⁸ 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 in their cars for discrete (and typically brief) periods of time, but carry their cell phones with them wherever they go, including to the most private spaces protected by the Fourth Amendment. *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

²⁸ *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 . . .”).

shower.”); *see also United States v. Powell*, 943 F. Supp. 2d 759, 777 (E.D. Mich. 2013). 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*, 152 So. 3d 504, 522 (Fla. 2014).

Second, acquisition of historical CSLI records constitutes a search irrespective of their duration. Like the tracking in *Karo*, CSLI reveals or enables the government to infer information about whether the cell phone is inside a constitutionally 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; *see also Riley*, 134 S. Ct. at 2490 (“Historic location information . . . can reconstruct someone’s specific movements down to

the minute, not only around town but also within a particular building.”); *United States v. Davis*, 754 F.3d 1205, 1216 (11th Cir. 2014) (“[T]he exposure of the cell site location information can convert what would otherwise be a private event into a public one.”), *vacated pending rehearing en banc*, 573 F. App’x 925 (mem.).

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’n 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. Carpenter’s cell phone records frequently indicate when he was home. *Supra* Part I.A.ii. 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 Supreme 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.

Moreover, the government’s own use of the records in this case belies any argument that they are imprecise. At trial the prosecution used Defendants’ CSLI to demonstrate that Mr. Carpenter was “right where the first robbery was at the exact time of the robbery, the exact sector,” (R333, Tr. 12/16/13, Page ID 3214), that he was “right in the right sector before the Radio Shack in Highland Park,” (*id.*), and the direction and timing of his movement to and from specific locations, (*id.*), among other information. (*See also* R332, Tr. 12/13/13, Page ID 3011–3024). Law enforcement combed through a combined 215 days of Defendants’ location records without a warrant and relied on the information to show where they were and what they were doing. When the government found 16 location data points that it believed corroborated its theory of the case, it asserted their accuracy and probativeness to the jury. (*See* Gov’t Trial Ex. 57, Appellant Carpenter’s App. 001–015; R.332, Tr. 12/13/13, Page ID 3011, 3014–3016, 3018, 3023; R333, Tr. 12/16/13, Page ID 3213–3214, 3269.) But it cannot be that the 35,932 remaining data points reveal nothing private about Defendants’ lives. *See* Exs. D & E. 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.

This Court's opinion in *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), is not to the contrary, and the district court's reliance on it was misplaced. (See R227, Op., Page ID 1216–1217). In *Skinner*, police, without a warrant, obtained real-time location information about a suspect's cell phone over a three-day period, while he was making a single multi-state car trip on public highways. 690 F.3d at 776. A divided panel of this Court held that the defendant “did not have a reasonable expectation of privacy in the location of his cell phone while traveling on public thoroughfares” because “that same information could have been obtained through visual surveillance.” *Id.* at 778. This case differs from *Skinner* in at least three determinative ways.

First, citing Justice Alito's concurrence in *Jones*, this Court in *Skinner* explained that “[t]here may be situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes.” *Id.* at 780 (citing *Jones*, 132 S. Ct. at 957–64). Tens of thousands of location points contained in hundreds of days of data constitute such comprehensive tracking. The *Jones* concurrences explained that at least longer-term electronic location tracking violates reasonable expectations of privacy, and although they did “not identify with precision the point at which the tracking of this vehicle became a search,” they noted that “the line was surely crossed before

the 4-week mark.” 132 S. Ct. at 964 (Alito, J.). That the three days of tracking in *Skinner* came “nowhere near that line,” 690 F.3d at 780, has no bearing on the outcome of this case. The four months of warrantlessly collected location data here clearly constitutes comprehensive tracking and is therefore an unreasonable search.

Second, the cell phone location data in *Skinner* revealed only the defendant’s movements on public roadways during a single trip. Defendants’ CSLI records here, however, reveal far more, including their presence inside their homes and other private spaces and their patterns of comings and goings over the course of months. As explained in *Karo*, people have a reasonable expectation of privacy in such information about location in protected spaces. 468 U.S. at 714–15; *see also Davis*, 754 F.3d at 1216. That information could not “have been obtained through visual surveillance.” *Skinner*, 690 F.3d at 778.

Finally, the information obtained by police in this case could not “have been obtained through visual surveillance,” *id.*, for another reason. 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. Police by definition could not have obtained the same information by visual observation 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 long-concluded movements and locations. *Jones*, 132 S. Ct. at 964 (Alito, J.).

Acquisition of historical CSLI is a search, and warrantless requests for it 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 has argued elsewhere that people have no reasonable expectation of privacy in their cell phone location information because that information was “voluntarily” conveyed to the service provider and contained in its business records. On the contrary, Defendants never voluntarily conveyed their location information to their wireless carriers, and the Supreme 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; *Davis*, 754 F.3d at 1216–17; *Tracey*, 152 So. 3d at 522–23; *see also Commonwealth v. Augustine*, 4 N.E. 3d 846, 863 (Mass. 2014) (analyzing question under state constitution); *State v. Earls*, 70 A.3d 630, 641 (N.J. 2013) (same); *accord United States v. Cooper*, No. 13-cr-00693-SI-1, 2015 WL 881578, at *8 (N.D. Cal. Mar. 2, 2015). That is the correct conclusion, and this Court should follow it here.

Older Supreme Court cases involving the so-called “third-party doctrine” do not reach the government surveillance at issue in this case. Those cases, *see United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979), have been overtaken by a host of Supreme Court decisions recognizing that in sharing information with the public or a third party, individuals do not necessarily surrender their expectation of privacy. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J.); *id.* at 964 (Alito, J.); *see also, e.g., Florida v. Jardines*, 133 S. Ct. 1409, 1418–19 (2013) (Kagan, J., concurring) (odors detectable by a police dog that emanate from a home); *Kyllo*, 533 U.S. 27 (thermal signatures emanating from a home); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (diagnostic-test results held by hospital staff). These cases confirm that an individual’s expectation of privacy in information does not hinge simply on whether she has shared it with another person.

But even taking the old third-party–records cases at face value, they do not apply here. In *Miller*, 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, 425 U.S. 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*, 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. 442 U.S. 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.

An individual’s expectation of privacy in cell phone location information thus turns, under this caselaw, 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 or receiving 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 Court held that 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 not actively, intentionally, or affirmatively disclosed by the caller.

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*, 152 So. 3d at 525–26 (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.²⁹

The fact that cell phone location information is handled by a third party is not dispositive. This Court's opinion in *United States v. Warshak*, 631 F.3d 266

²⁹ 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.

(6th Cir. 2010), is instructive. There, this Court held that there is a reasonable expectation of privacy in the contents of emails. This 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 phone calls and letters are sent via third parties (phone companies and the postal service), 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. 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). 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. In this case the government obtained a transcript of two individuals' locations and movements over a

staggering 127 and 88 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.). 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*, 152 So. 3d at 523.

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 to the exclusionary rule applies.³⁰ When a case presents a “novel question of law whose

³⁰ Without elaboration or factual findings, the district court incorrectly concluded that the good-faith exception applies. (R227, Op., Page ID 1216 n.1). *Amici* agree with Defendants that the good-faith exception should not apply. Carpenter’s Br. 34–38.

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 requests are already used far more frequently than the GPS tracking technology in *Jones*. Their highly intrusive nature cries out for clear judicial regulation.

In *Warshak*, this Court 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 cell phone location records by police. Phone companies have been inundated with law enforcement requests for location data in recent years: in 2014, for example,

AT&T received 64,073 requests for cell phone location information.³¹ As the use of cell phones becomes near-universal and CSLI 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 before this Court, and addressing it would yield much needed clarity in this Circuit.

CONCLUSION

This Court should hold that under the Fourth Amendment a warrant is required for collection of CSLI.

³¹ AT&T, *Transparency Report 4* (2015), available at http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_January_2015.pdf.

Respectfully Submitted,

Dated: March 9, 2015

By: /s/ Nathan Freed Wessler

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

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
American Civil Liberties Union Fund
of Michigan
2966 Woodward Ave.
Detroit, MI 48201
(313) 578-6800

Rachel Levinson-Waldman
Michael W. Price
Brennan Center for Justice at NYU
School of Law
161 Avenue of the Americas,
12th Floor
New York, NY 10013
(646) 292-8335
rachel.levinson.waldman@nyu.edu
michael.price@nyu.edu

Gregory T. Nojeim
Center for Democracy and
Technology
1634 Eye St., NW
Suite 1100
Washington, DC 20006
(202) 637-9800

Hanni Fakhoury
Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
hanni@eff.org

Kristina W. Supler, Esq.
Vice Chair, 6th Circuit, Amicus
Committee
National Association of Criminal
Defense Lawyers
McCarthy, Lebit, Crystal &
Liffman Co., L.P.A.
101 Prospect, W., Suite 1800
Cleveland, Ohio 44115-1088
Phone: (216) 696-1422, Ext. 273
Facsimile: (216) 696-1210
kws@mccarthylebit.com

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a) because it contains 7,000 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

March 9, 2015

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 9th day of March, 2015, the foregoing Amici Curiae Brief for the American Civil Liberties Union, the American Civil Liberties Union of Michigan, the Brennan Center for Justice, 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

DESIGNATION OF RELEVANT DISTRICT COURT DOCUMENTS

Description of Entry	Record Entry Number	Page ID Range
Application and Order for cell site location information	221-2	1141–1152
Application and Order for cell site location information	221-3	1153–1163
Application and Order for cell site location information	221-4	1164–1174
Opinion & Order	227	1213–1224
Trial Transcript, Dec. 13, 2013, Testimony of Special Agent Christopher Hess	332	2994–3064; 3067–3087
Trial Transcript, Dec. 16, 2013, Government's Closing Argument	333	3213–3214; 3269