Linda Lye (CA SBN 215584)
llye@aclunc.org
Nicole Ozer (CA SBN 228643)
nozer@aclunc.org
Christopher J. Conley (CA SBN 290747)
cconley@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street, 2nd Floor
San Francisco, California 94111
Tel.: (415) 621-2493
Fax: (415) 255-8437

ATTORNEYS FOR *AMICUS* AMERICAN CIVIL
LIBERTIES UNION OF NORTHERN CALIFORNIA

Nathan Freed Wessler
nwessler@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 549-2500
Fax: (212) 549-2654

ATTORNEYS FOR *AMICUS*
AMERICAN CIVIL LIBERTIES UNION

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: APPLICATION FOR TELEPHONE INFORMATION NEEDED FOR CRIMINAL INVESTIGATION	CASE No.: CR 15-XR-90304-HRL-1 (LHK) **BRIEF *AMICI CURIAE* OF AMERICAN CIVIL LIBERTIES UNION AND AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA IN SUPPORT OF FEDERAL PUBLIC DEFENDER**

TABLE OF CONTENTS

I. SUMMARY OF ARGUMENT 1
II. BACKGROUND 2
A. Overview of Cell Site Location Technology 2
B. CSLI Can Reveal Private, Invasive, and Increasingly Precise Information About Individuals' Locations and Movements 4
III. ARGUMENT 7
A. Long-Term Location Tracking Is a Search Under the Fourth Amendment Requiring a Warrant Based Upon Probable Cause 7
B. Cell Phones Providers' Ability to Access Customers' Location Data Does Not Eliminate Cell Phone Users' Reasonable Expectations of Privacy in That Data 10
C. A Bright-Line Warrant Requirement Is Necessary 16
IV. CONCLUSION 18

TABLE OF AUTHORITIES

Cases

Commonwealth v. Augustine, 4 N.E. 3d 846 (Mass. 2014) 13

Couch v. United States, 409 U.S. 322 (1973) 11

DeMassa v. Nunez, 770 F.2d 1505 (9th Cir. 1985) 14

Ferguson v. City of Charleston, 532 U.S. 67 (2001) 12

Florida v. Jardines, 133 S. Ct. 1409 (2013) 12

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) 10

Katz v. United States, 389 U.S. 347 (1967) 7

Kyllo v. United States, 533 U.S. 27 (2001) 9, 10, 12, 18

New York v. Belton, 453 U.S. 454 (1981) 17

Riley v. California, 134 S. Ct. 2473 (2014) 15, 17

See v. City of Seattle, 387 U.S. 541 (1967) 10

Smith v. Maryland, 442 U.S. 735 (1979) ..... *passim*

State v. Earls, 70 A.3d 630 (N.J. 2013) 13, 16

Stoner v. California, 376 U.S. 483 (1964) 10

Tracey v. State, 152 So. 3d 504 (Fla. 2014) ..... *passim*

Tucson Woman's Clinic v. Eden, 379 F.3d 531 (9th Cir. 2004) 12

United States v. Cooper, No. 13-cr-00693-SI-1, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015) 13, 16

United States v. Davis, 785 F.3d 498 (11th Cir. 2015) 11, 13, 14, 15

United States v. Forrester, 512 F.3d 500 (9th Cir. 2007) 12

United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108 (9th Cir. 2012) 12

United States v. Karo, 468 U.S. 705 (1984) 9

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012) 1, 12, 18

United States v. Miller, 425 U.S. 435 (1976) 11, 13, 14

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) 12

United States v. Wurie, 728 F.3d 1 (1st Cir. 2013) 17

Other Authorities

3rd Generation Partnership Project 2, *Femtocell Systems Overview* (2011) 4

CTIA – The Wireless Ass'n, *Annual Wireless Industry Survey* (2014) 2

CTIA –The Wireless Ass'n, *Semi-Annual Wireless Industry Survey* (2012) 4

Ctr. for Democracy & Tech., Cell Phone Tracking: Trends in Cell Site Precision (2013) 4

Gyan Ranjan, et al., *Are Call Detail Records Biased for Sampling Human Mobility* 3

Letter from Charles W. McKee, Vice President, Sprint Nextel, to Hon. Edward J. Markey (Oct. 3, 2013) 3

Letter from Timothy P. McKone, Executive Vice President, AT&T, to Rep. Edward J. Markey (Oct. 3, 2013) 3

Maeve Duggan & Lee Rainie, Pew Research Ctr., *Cell Phone Activities 2012* (2012) 3

Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Ctr., 32, 34 (2014) 16

MetroPCS, MetroPCS Subpoena Compliance 3

Pew Research Ctr., *Mobile Technology Fact Sheet* (Jan. 2014) 2

Stephen J. Blumberg & Julian V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January–June 2014*,Ctr. For Disease Control & Prevention (2014) 2

Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681 (2011) 3

The Electronic Communications Privacy Act (ECPA)(Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. on the Judiciary, 113th Cong. 50 (2013) 2

Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Attorneys' Bull., Nov. 2011 3

Verizon Wireless Law Enforcement Resource Team (LERT) Guide (2009) 3

I. 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*, in which the government tracked an investigative suspect's vehicle for 28 days without a warrant, five Justices of the Supreme Court concluded that his "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." 132 S. Ct. at 958 (Alito, J., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring).

In this case, law enforcement seeks to obtain, without a warrant, 60 days of historical cell site location information ("CSLI") for several cell phones. If tracking a vehicle for 28 days in *Jones* was a search, then tracking several cell phones for over twice that period is likewise a search. Indeed, the information at issue here is even more revealing than in *Jones* because people keep their phones with them when they leave their vehicles and enter private spaces traditionally and robustly protected by the Fourth Amendment. The magistrate judge correctly reasoned that 60 days of historical CSLI constitutes a Fourth Amendment search for which a warrant is required. This court should affirm.

CSLI can provide a detailed accounting of a person's movements and reveal political, religious, and romantic affiliations. Cell phone users have a reasonable expectation of privacy in this deeply sensitive information. This is so even though the information is contained in records collected by third-party service providers because cell phone users do not voluntarily convey their location information to their providers. Finally, a warrant requirement cannot and should not turn on the precision of the data at issue in a particular case. A bright-line rule requiring a

warrant to acquire CSLI is necessary to provide courts, law enforcement, and the public with consistent and workable rules.

II. BACKGROUND

A. Overview of Cell Site Location Technology

As of December 2013, there were 335.65 million active wireless devices in the United States, responsible for 2.62 trillion annual minutes of calls and 1.91 trillion annual text messages.[1] Cell phone use has become ubiquitous: more than 90% of American adults own cell phones[2] and 44% of U.S. households have only wireless telephones.[3]

Cellular telephones regularly communicate with the carrier's network by sending radio signals to nearby base stations, or "cell sites."[4]

CSLI can provide a detailed accounting of a person's whereabouts, but the level of precision turns on a variety of factors, including the type of information the service provider retains about such information, the frequency with which the phone communicates with the network, and the density and type of cell towers in the area.

Type of information retained. When phones communicate with the network, the service provider's equipment generates records about that communication, which the provider typically retains.[5] These records may include not only the location of the cell tower to which the phone

---

[1] 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.

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

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

[4] *The Electronic Communications Privacy Act (ECPA)(Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 50 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) [hereinafter *Blaze Hearing Statement*], *available at* http://fas.org/irp/congress/2013_hr/ecpa2.pdf.

[5] 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

connected but also additional information about the direction of the phone relative to the antenna (known as the cell site "sector")[6] and even the distance from the cell site.[7]

Frequency. Modern cellular phones communicate with the network in a variety of circumstances. "Cell 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."[8] Smartphones, which are now used by a majority of Americans,[9] communicate more frequently with the network than traditional "feature" phones. Connections to the network are triggered not only by user-initiated activities such as placing voice-calls and sending text messages but also by passively receiving calls and text messages and by data activities that require no user initiation, nor even participation, such as "push-mail notifications, periodic software updates and weather services, to name a few."[10]

(Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf; Letter from Charles W. 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.

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

[7] *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).

[8] *Blaze Hearing Statement*, *supra* note 4, at 50.

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

[10] Gyan Ranjan, et al., *Are Call Detail Records Biased for Sampling Human Mobility*, *available at* http://www-users.cs.umn.edu/~granjan/Reports/MC2R_2012_CDR_Bias_Mobility.pdf; *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 703 (2011) ("Although the frequency of such [passive network] connections may vary by provider and change over time, it appears that they are made as frequently as every seven seconds.").

Density and type of cell towers. The precision of the location data also turns on the density of cell towers and antennae in the vicinity, with more precise location available in urban areas where there are more cell towers.

Cell site density is increasing rapidly, largely as a result of the growth of Internet usage by smartphones. The number of cell sites in the United States has more than doubled in the last decade, with wireless data traffic having increased by almost 500% between 2009 and 2012.[11] Each cell site can supply a fixed bandwidth of data required for text messages, emails, web browsing, streaming video and other uses. Therefore, the only way for providers to maintain adequate coverage as smartphone data usage increases is to erect more cell sites. As new cell sites are erected, the coverage areas around existing nearby cell sites will be reduced, so that the signals sent by those sites do not interfere with each other.[12] Many of these new sites consist of low-power small cells, called "microcells," "picocells," and "femtocells," which provide service to areas as small as ten meters.[13] Callers connecting to a carrier's network via such cells thus can be located to a high degree of precision, "sometimes effectively identifying individual floors and rooms within buildings."[14]

B. CSLI Can Reveal Private, Invasive, and Increasingly Precise Information About Individuals' Locations and Movements

In its Order for Response and Continuing Hearing, the Court expressed its interest in the precision of the CSLI sought by the government in this case. *See* ECF No. 7.

---

[11] *See* CTIA –The Wireless Ass'n, *Semi-Annual Wireless Industry Survey* (2012) (285,561 cell sites as of June 2012), *available at* http://files.ctia.org/pdf/CTIA_Survey_MY_2012_Graphics-_final.pdf.

[12] *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.

[13] *Id.*

[14] *Blaze Hearing Statement*, *supra* note 4, at 56. 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.

A completely accurate answer cannot be supplied at this juncture because the precision of the location information will turn on factors that cannot be ascertained without first collecting and reviewing the data. For example, it is impossible to know now (a) if the target cell phones were used during the 60-day period at issue here in sparsely populated rural areas or in urban areas with a high density of cell sites consisting of femtocells or geographically small sectors of convention cell towers; (b) whether the carrier(s)'s records include information not only about the cell tower to which the phones connected but also the direction and distance from the cell site; and (c) how frequently the target cell phones communicated with the network.

Nevertheless, the available information suggests that the CSLI sought in this case is likely to be extremely revealing.

Examples from other cases in urban areas are instructive. In *United States v. Carpenter*, a case now pending in the Sixth Circuit and arising out of the greater Detroit area, the government obtained 127 days of CSLI for one defendant, Timothy Carpenter, and 88 days of records for another, Timothy Sanders. *United States v. Carpenter*, Case No. 14-1572 (6th Cir. filed May 7, 2014). Mr. Carpenter's data include 6,449 separate call records for which CSLI was logged, comprising 12,898 cell site location data points.[15] *See* Wessler Decl. at ¶ 8. Mr. Sanders's records reveal 11,517 calls for which location information was logged, comprising 23,034 cell site location data points. *Id.* at ¶ 9. Mr. Carpenter and Mr. Sanders, respectively, 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. *Id.* at ¶ 10. For Mr. Carpenter, that amounts to an average of 102 location points per day, or one location point every 14 minutes. For Mr. Sanders, it amounts to an average of 262 location points per day, or one location point every six minutes.

The number of location points in this case will vary depending on, among other things, the number of calls or texts placed or received by the suspects. But if the *Carpenter* data serve as

[15] 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. *Id.* at ¶ 8.

any benchmark, the government here is effectively seeking to track the suspects' location and movements every six to fourteen minutes for a 60-day period.

The *Carpenter* data also illustrate how the type of records sought by the government can provide a granular accounting of individuals' movements, as well as intimate details about the locations they visit.

Call records of the type sought here can chart an individual's movements not only over the course of the entire period during which the data is collected, but also over the course of individual days and even during individual phone calls. For example, Mr. Carpenter's calls show his location in more than 200 separate cell site sectors. *Id.* at ¶ 11. On one day, Mr. Carpenter made and received 141 calls while located in 40 unique sectors. *Id*. Hundreds of his calls were initiated within one cell site sector and terminated in another, suggesting that he moved from one location to another during the call. *Id.* at ¶ 12.

The records at issue here can also provide strong indications of when an individual was at home, when he left, and when he returned. During one two-week period, 117 of Mr. Carpenter's calls were placed or received while he was located in the cell site and sector closest to his home. Of those calls, 11 started in his home sector and ended elsewhere, and seven started elsewhere and ended in his home sector. *Id.* at ¶ 14.

The records also provide insight into an individual's religious, political, or other affiliations. Mr. Carpenter attended church during the period he was monitored, and indeed the call records show that he made or received calls from sectors overlapping with his church in the early afternoon on a number of Sundays. *Id.* at ¶ 15. His records reflect that his phone was not routinely located in those sectors at other times of the week, leading to a strong inference about his patterns of worship.

Further, the records here can allow inferences about where individuals sleep, which in turn can reveal private information about relationships and infidelities. By sorting the data for the first and last calls of each day, one can infer whether a person slept at home or elsewhere. During one five-day period, Mr. Carpenter's last call of the night and/or first call of the morning were

from his home sector. But on the immediately preceding night, the last call of the night and first call of the next morning were placed from overlapping sectors approximately four miles from his home. *Id.* at ¶ 16.

While the particularities of the information sought by the government in this case cannot yet be ascertained, there can be no doubt that the records are capable of revealing detailed information that is deeply sensitive and quintessentially private.

III. ARGUMENT

A. Long-Term Location Tracking 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. *See generally Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (search occurs where government intrudes on "reasonable expectation of privacy"). Acquisition of cell phone location information is a search for these two independent reasons, which we discuss in turn.

First, five Justices in *United States v. Jones* 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., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring).

Jones 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 947. 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* 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., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring). 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 (quoting *United States v. Cuevas–Perez*, 640 F.3d 272, 285 (C.A.7 2011) (Flaum, J., concurring)).

Pursuant to the views of five Justices in *Jones*, acquisition of at least longer-term CSLI without a warrant violates the Fourth Amendment. If tracking a car's location for 28 days violates an expectation of privacy that society is prepared to recognize as reasonable, then tracking a cell phone's location for 60 days necessarily does as well. 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., concurring in the judgment), so, too, is it society's expectation that government agents would not track the location of one's cell phone for 60 days. Such tracking can reveal intimate details about a person's movements, as well as political, religious, and romantic affiliations. *See supra* Part II-B.

Recent disclosures about widespread warrantless surveillance have reinforced the societal demand for privacy of personal information. A recent survey by the Pew Internet & American Life project found that nine out of ten adults say that controlling who can access their personal information and/or what information is collected is important.[16] Eighty-two percent of

[16] Mary Madden and Lee Rainie, *Americans' Views about Data Collection and Security*, Pew Research Ctr. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security/.

Americans consider the "details of [their] physical location over time" to be "sensitive."[17] The vast majority of Americans expect and deserve privacy in their historical location information. Historical CSLI 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) (internal quotation marks omitted).

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

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 carry their cell phones with them

[17]Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Ctr., 7 (2014), *available at* http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

wherever they go, including their homes and other private locations, as reflected for example in the data in *Carpenter* and other cases. Like the tracking in *Karo*, CSLI thus reveals or enables the government to infer information about whether the cell phone is inside constitutionally protected locations, where individuals enjoy reasonable expectations of privacy and the government is prohibited from intruding without a warrant. *See Karo*, 468 U.S. at 714; *see also, 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, 489 (1964) (hotel room); *Tracey*, 152 So. 3d at 524 ("[B]ecause cell phones are indispensable to so many people and are normally carried on one's person, cell phone tracking can easily invade the right to privacy in one's home or other private areas.").

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) [hereinafter *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. Moreover, the rapid proliferation of cells, including short-range cells, means that CSLI information may match the precision of GPS information.[18]

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

Because cell phone users do not voluntarily convey their location information to their wireless carriers, the Supreme Court's business records cases do not extend to the scenario presented here. Numerous appellate courts and another court of this district agree. The government contends that voluntariness is irrelevant where, as here, the service provider chooses

[18] *Blaze Hearing Statement*, *supra* note 4, at 53.

to keep the records, and that cell phone users do, in any event, convey the information voluntarily. The government is wrong on both counts. *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), both confirm that voluntariness is an essential component of the analysis, and the Eleventh Circuit's recent decision in *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015), rests on flawed reasoning which this Court should reject.

1. The third-party doctrine does not apply here because CSLI is not voluntarily communicated to a service provider.

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. 425 U.S. at 437. The Court observed that the documents were the bank's business records and rejected a property-based argument that the defendant had a Fourth Amendment interest in the records. 425 U.S. at 440. Instead, it focused on the core question of whether the information at issue implicates a reasonable privacy expectation: "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 (quoting *Couch v. United States*, 409 U.S. 322, 335 (1973)). 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*, 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 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. Thus, *Smith,* like *Miller,* analyzed voluntary conveyance. In addition, the Court also assessed the degree of invasiveness of the surveillance at issue to determine whether the user had a reasonable expectation of privacy. *See id.* at 741-42 (noting a "pen register's limited capabilities").

Further, more recent Supreme Court cases recognize that individuals do not necessarily

surrender their expectation of privacy, even in activities or information an individual exhibits to the public. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (GPS tracking); *id.* at 964 (Alito, J., concurring in the judgment); *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). Other cases also recognize that an individual can enjoy a reasonable expectation of privacy in records held by a third party. *See Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (reasonable expectation of privacy in diagnostic test results held by hospital staff); *United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108, 1116 (9th Cir. 2012) (explaining that records held by a third party that are "more inherently personal or private than the bank records in *Miller*" may receive Fourth Amendment protection, and listing "the personal nature of Google search queries" stored by that company as an example); *United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010) (expectation of privacy in emails stored by service provider); *Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 550 (9th Cir. 2004) (expectation of privacy in records held by abortion services); *see also United States v. Forrester*, 512 F.3d 500, 510, 511 (9th Cir. 2007) (finding no expectation of privacy in IP addresses of websites visited because users should know that they relay this information to their internet service providers, but expressly clarifying that court's holding "does not imply that more intrusive techniques or techniques that reveal more content information are also" governed by *Smith*).

The case law makes clear that an individual's expectation of privacy in cell phone location information 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 317-18 (last alteration in original). Other appellate courts and a court of this district agree that users maintain a reasonable expectation of privacy in their location information, even though that information can be accessed by a third party business. *See 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).

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.

Finally, many smartphones include a location privacy setting that, when enabled, prevents applications from accessing the phone's location. But this setting has no impact upon carriers' ability to learn the cell sector in use. In other words, CSLI is not actively, intentionally, or affirmatively disclosed by the caller.

2. Although the Eleventh Circuit in *Davis* concluded that cell phone users lack a reasonable expectation of privacy in CSLI, *amici* respectfully contend that the court's reasoning was flawed and should be rejected here.

First, *Davis* emphasizes, as does the government, that the records belong to the carrier,

and not the cell phone user. *See Davis*, 785 F.3d at 511; Gov't Appeal at 4 (ECF No. 4). Possession would be dispositive if the Fourth Amendment analysis turned solely on property rights, but it does not. *See, e.g.*, *DeMassa v. Nunez*, 770 F.2d 1505, 1507 (9th Cir. 1985) ("[I]t is clear that neither ownership nor possession is a necessary or sufficient determinant of the legitimacy of one's expectation of privacy."). As noted above, the Supreme Court in *Miller* observed that the records belonged to the bank in the context of rejecting the defendant's argument that the records constituted his private papers. 425 U.S. at 440. *Miller* nowhere identified record ownership as dispositive of the separate *Katz* analysis. *Id.* at 442-43. And the implications of such an approach would be staggering. "Under a plain reading of the [*Davis*] majority's rule, by allowing a third-party company access to our e-mail accounts, the websites we visit, and our search-engine history—all for legitimate business purposes—we give up any privacy interest in that information. And why stop there? . . . . [U]nder the majority's rule, the Fourth Amendment allows the government to know from YouTube.com what we watch, or Facebook.com what we post or whom we 'friend,' or Amazon.com what we buy, or Wikipedia.com what we research, or Match.com whom we date—all without a warrant." *Davis*, 785 F.3d at 536 (Martin, J., dissenting).

Second, and relatedly, *Davis* and the government stress that cellular carriers keep the records by choice, and not under government compulsion. *See Davis*, 785 F.3d at 512; Gov't Appeal at 4, 7 (ECF No. 4). Both *Miller* and *Smith* reject the relevance of such factors. In *Miller*, the Court expressly held that the analysis of whether the defendant had a reasonable expectation of privacy in his bank records "is not changed by the mandate of the Bank Secrecy Act that records of depositors' transactions be maintained by banks." 425 U.S. at 443. And in *Smith*, the defendant contended that he had a reasonable expectation of privacy because, under then-prevailing billing practices, phone companies did not typically keep records of the type of phone call he had made. 442 U.S. at 745. The Supreme Court in *Smith* summarily rejected this line of reasoning: "The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not, in our view, make any constitutional

difference." *Id.* "Regardless of the phone company's election," the central question, the Court explained, is whether the defendant "voluntarily conveyed" the information. *Id.* The Supreme Court has foreclosed the government's assertion in this case, that the voluntariness inquiry is triggered by the third party's record-keeping choices. *Cf.* Gov't Appeal at 7 (ECF No. 4). "We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where . . . the pattern of protection would be dictated by billing practices of a private corporation." *Smith*, 442 U.S. at 745.

Third, the *Davis* court suggested that the information in *Smith* was more intrusive than cell site records because the stationary landlines in use at the time corresponded to physical addresses. *Davis*, 785 F.3d at 511-12. *Davis* is correct that the intrusiveness of the surveillance informs the *Katz* analysis, but it erred in describing a pen register as more intrusive than CSLI. *Smith* itself emphasized the "limited capabilities" of a pen register, which does not reveal such basic information as the "identities" of caller or recipient, "nor whether the call was even completed." 442 U.S. at 741. As the facts discussed above demonstrate, CSLI provides comprehensive information on where and when an individual comes and goes, tracking her movements every few minutes over the course, in this case, of a proposed two month period, and shedding light on religious affiliations, infidelities, and other intimate details. *See Davis*, 785 F.3d at 540 ("The amount and type of data at issue revealed so much information about Mr. Davis's day-to-day life that most of us would consider quintessentially private.") (Martin, J., dissenting). While the landline phones of yore were constrained in functionality and portability, cell phones are used nearly constantly for calls, text messages, and data connections, and "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014).

Finally, *Davis* at root turned on the court's conclusion that cell phone users knowingly, and therefore voluntarily, convey their location information to their service providers. 785 F.3d at 511. But even if some people are now aware that service providers log CSLI, 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 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.[19]

Numerous appellate courts and another court of this district have found that cell phone users may maintain a reasonable expectation of privacy in their location information. *See Third Circuit Opinion*, 620 F.3d at 317–18; *Tracey*, 152 So. 3d at 522–23; *see also Augustine*, 4 N.E. 3d at 863 (Massachusetts constitution); *Earls*, 70 A.3d at 641 (New Jersey constitution); *accord Cooper*, No. 13-cr-00693-SI-1, 2015 WL 881578, at *8. That is the correct conclusion and the Court should follow it here.

C. A Bright-Line Warrant Requirement Is Necessary

In its Order for Response and Continuing Hearing, the Court expressed an interest in the precision of the requested CSLI. *See* ECF No. 7. CSLI is indeed precise and, for that reason, cell phone users have a reasonable expectation of privacy in such information. But the Fourth Amendment inquiry cannot turn on the precision of the data returned in each individual case. Rather, a bright-line rule is necessary for two reasons.

First, in the context of the Fourth Amendment, the Supreme Court has eschewed fact-specific inquiries in favor of bright-line rules that clearly delineate whether a given activity is or

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

is not a search under the Fourth Amendment. *See United States v. Wurie*, 728 F.3d 1, 12-13 (1st Cir. 2013), *aff'd sub nom. Riley v. California*, 134 S. Ct. 2473 (2014). This preference is driven both by an interest in providing law enforcement officers and courts with workable rules that produce consistent results and with the need to clearly inform the public of the extent of their constitutional rights. *See id.*; *New York v. Belton*, 453 U.S. 454, 459-60 (1981). In addition, the Supreme Court has endorsed bright-line rules where the alternative would "launch courts on a difficult line-drawing expedition" that "would keep defendants and judges guessing for years to come." *Riley*, 134 S. Ct. at 2493.

Second, the Fourth Amendment mandate for a bright line rule is particularly necessary in the context of CSLI because the relevant facts to determine whether a demand for CSLI crosses some constitutional threshold are inherently unknowable at the time an order or warrant for such information is obtained. The number of records returned and the information they retain depends upon exactly how and where the phone was used over the relative time period. *See supra* Part II-A. Neither law enforcement nor the court will 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 a result, if the constitutionality of a demand for CSLI turned on the quantity or precision of information returned in a particular instance, no one would "be able to know *in advance* whether [the] surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." *Kyllo*, 533 U.S. at 39; *accord United States v. Powell*, 943 F. Supp. 2d 759, 775-76 (E.D. Mich. 2013) (applying *Kyllo* to cell site location information). As a result, a fact-specific analysis of the invasiveness of a particular demand for CSLI simply cannot be conducted at the time a court reviews an application.

IV. CONCLUSION

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. 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., concurring); *id.* at 963-64 (Alito, J., concurring in the judgment). 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 (citation omitted). The Court should affirm the magistrate's decision.

Dated: June 12, 2015

Respectfully Submitted,

By: ___/s/ *Christopher Conley* _____

Christopher Conley

Linda Lye
Nicole Ozer
Christopher Conley
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street, 2nd Floor
San Francisco, California 94111
Tel.: (415) 621-2493
Fax: (415) 255-8437

Attorneys for *Amicus* American Civil Liberties Union of Northern California

Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 549-2500
Fax: (212) 549-2654

Attorneys for *Amicus* American Civil Liberties Union