No. 16-10109

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

ANTONIO GILTON, *et al.*,

Defendants-Appellees.

On Appeal from the United States District Court
for the Northern District of California
No. 13-CR-00764-WHO-1

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, BRENNAN CENTER FOR JUSTICE, CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE IN SUPPORT OF DEFENDANT-APPELLANT SEEKING AFFIRMANCE

Linda Lye
American Civil Liberties Union
Foundation of Northern California
39 Drumm Street, 2nd Floor
San Francisco, California
(415) 621-2493

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

Additional counsel listed on next page

Gregory T. Nojeim
Center for Democracy and Technology
1401 K St., NW
Suite 200
Washington, DC 20005
(202) 637-9800
gnojeim@cdt.org

David M. Porter
Co-chair, NACDL Amicus Curiae Committee
National Association of Criminal Defense Lawyers
801 I Street, 3rd Floor
Sacramento, California 95814
(916) 498-5700

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

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

Kevin S. Bankston
Ross Schulman
New America's Open Technology Institute
740 15th St., N.W., Suite 900
Washington, DC 20005
(202) 986-2700

CORPORATE DISCLOSURE STATEMENT

Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Northern California, Brennan Center for Justice, Center for Democracy & Technology, Electronic Frontier Foundation, National Association of Criminal Defense Lawyers, and New America's Open Technology Institute are non-profit entities that do not have parent corporations. No publicly held corporation owns 10 percent of more of any stake or stock in *amici curiae*.

/s/ Nathan Freed Wessler

Nathan Freed Wessler

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF AMICI CURIAE[1]

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 Northern California is an 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 Northern California 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 Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice. 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 intelligence gathering policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms. As part of its work in this area, the Center has filed numerous *amicus*

[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.

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); *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *petition for cert. docketed*, No. 16-402 (Sept. 28, 2016); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016), *petition for cert. docketed*, No. 16-263 (Aug. 30, 2016); *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197 (2d Cir. 2016), *petition for reh'g* en banc *filed*, No. 14-2985 (Oct. 17, 2016); *United States v. Moalin*, No. 13-50572 (9th Cir. filed Nov. 5 2015); and *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015).

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized Internet. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of Internet users. 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. Graham*, 824 F.3d 421 (4th Cir. 2016); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015); *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. Commc'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 lawyers to ensure justice and due process for persons accused of crime or other misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands, and up to 40,000 attorneys including affiliates' members. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is an affiliated organization with representation in the ABA House of Delegates. NACDL is dedicated to advancing

the proper, efficient and just administration of justice and files numerous amicus briefs each year in federal and state courts addressing issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system.

New America's Open Technology Institute ("OTI") is New America's program dedicated to ensuring that all communities have equitable access to digital technology and its benefits, promoting universal access to communications technologies that are both open and secure. New America is a Washington, DC-based think tank and civic enterprise committed to renewing American politics, prosperity, and purpose in the Digital Age through big ideas, bridging the gap between technology and policy, and curating broad public conversation. New America's OTI has a special interest in preserving the privacy of all people who use modern technology, including cell phones, as evidenced by the complaint submitted to the Federal Communications Commission about police department use of so-called Stingray devices which enable geographic tracking of cell phones as well as content interception.

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. *See United States v. Reyes*, 435 F. App'x 596, 598 (9th Cir. 2011) ("The government's use at trial of Reyes's cell site location information raises important and troublesome privacy questions not yet addressed by this court."). *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* Fed. R. App. P. 29(g).

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 37 days 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 even longer 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 correctly concluded that people have a reasonable expectation of privacy in their historical cell site location information held by a service provider, and thus that a valid search warrant is required. This Court should

reject the government's reliance on factually distinguishable, four-decades-old Supreme Court cases 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). In contrast to the willful communication of banking transaction data and dialed numbers to banks and telecommunication companies, cell phone location data is not voluntarily communicated to cellular service providers. The government's acquisition of Defendants' comprehensive cell phone location information without a warrant violates the Fourth Amendment.

ARGUMENT

I. Gilton's CSLI Obtained by the Government Reveals Invasive and Detailed Information About His Location and Movements Over Time.

A. CSLI reveals private, invasive, and increasingly precise information about individuals' locations and movements.

As of December 2015, there were more than 377 million wireless subscriber accounts in the United States, responsible for 2.88 trillion annual minutes of calls and 1.89 trillion annual text messages.[2] Cell phone use has become ubiquitous:

[2] CTIA – The Wireless Ass'n, *Annual Wireless Industry Survey* (2016), http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

more than 90% of American adults own cell phones[3] and 48% of U.S. households have only wireless telephones.[4]

Cellular telephones regularly communicate with the carrier's network by sending radio signals to nearby base stations, or "cell sites."[5] When turned on, "[c]ell phone handsets periodically (and automatically) identify themselves to the nearest base station (that with the strongest radio signal) as they move about the coverage area."[6] When phones send or receive calls or text messages, the service provider's equipment generates records about that communication, which the provider typically retains.[7] Smartphones, which are now used by almost seven in

---

[3] Pew Research Ctr., *Technology Device Ownership: 2015* (2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

[4] CTIA – The Wireless Ass'n, *Annual Wireless Industry Survey*, *supra*.

[5] *The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary*, 113th Cong. 6 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) ["Blaze Hearing Statement"], https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf.

[6] *Id.*

[7] 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. Letter from Timothy P. McKone, Executive Vice President, AT&T, to Rep. Edward J. Markey 3 (Oct. 3, 2013), 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), http://s3.documentcloud.org/documents/889100/response-sprint.pdf.

ten Americans,[8] communicate even more frequently with the carrier's network, because they typically check for new email messages or other data every few minutes.[9] For each incoming and outgoing call, service providers log the cell site the phone was connected to at the beginning and end of the call, as well as the "sector" of that cell site.[10] Cell site and sector information are also recorded when a phone sends or receives a text message or makes a data connection with the network; during data sessions ("such as checking email, watching a video, or using apps"), the service provider may collect "multiple location points."[11] Most cell sites consist of three directional antennas that divide the cell site into sectors (usually of 120 degrees each),[12] but an increasing number of towers have six

[8] Pew Research Ctr., *supra*.

[9] Gyan Ranjan et al., *Are Call Detail Records Biased for Sampling Human Mobility?*, 16 Mobile Computing & Comm. Rev. 33, 34 (2012), http://www-users.cs.umn.edu/~granjan/Reports/MC2R_2012_CDR_Bias_Mobility.pdf.

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

[11] Craig Silliman, Exec. Vice President, Pub. Pol'y & Gen. Counsel, Verizon, *Technology and Shifting Privacy Expectations*, Bloomberg Law, Oct. 7, 2016, https://bol.bna.com/technology-and-shifting-privacy-expectations-perspective/.

[12] Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, 59 U.S. Attorneys' Bull. 16, 19 (2011), http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

sectors. In addition to cell site and sector, carriers can also calculate and log the caller's distance from the cell site.[13]

The precision of a user's location revealed by the cell site records depends on the size of the sector. The coverage area for a cell site is smaller in areas with greater density of cell towers, with urban areas having the greatest density and thus the smallest coverage areas.[14]

Cell site density is increasing rapidly, largely as a result of the growth of data usage by smartphones. *See* CTIA, *Annual Wireless Industry Survey*, *supra* (showing that the number of cell sites in the United States increased from 183,689 to 307,626 from 2005 to 2015); *id.* (annual wireless data usage increased from 388 billion megabytes to 9.65 trillion megabytes between 2010 and 2015). Each cell site can supply a fixed volume of data required for text messages, emails, web browsing, streaming video, and other uses. Therefore, as smartphone data usage increases, carriers must erect additional cell sites, each covering smaller geographic areas. As new cell sites are erected, the coverage areas around existing nearby cell sites will be reduced, so that the signals sent by those sites do not interfere with each other.[15] "In all, the dramatic increase in smart phones and data

[13] Silliman, *Technology and Shifting Privacy Expectations*, *supra*.

[14] Blaze Hearing Statement, *supra*, at 10–12.

[15] *See* Pell & Soghoian, *supra*, at 127.

usage means there is also a sizeable increase in customer location information generated by [a service provider's] network."[16]

In addition to erecting new conventional cell sites, providers are also increasing their network coverage using low-power small cells, called "microcells," "picocells," and "femtocells" (collectively, "small cells"), which provide service to much smaller areas.[17] These devices are often provided for free to consumers who complain about poor cell phone coverage in their homes or offices. The number of small cells nationally now exceeds the number of traditional cell sites.[18] Because the coverage area of these devices is so small, callers connecting to a carrier's network via small cells can be located to a high degree of precision, "sometimes effectively identifying individual floors and rooms within buildings."[19] Small cells with ranges extending outside of the building in

---

[16] Silliman, *Technology and Shifting Privacy Expectations*, *supra.*

[17] *Id.*

[18] *Compare* Michael Carroll, *Small Cells Hit Milestone*, FierceWireless, Nov. 1, 2012, http://www.fiercewireless.com/europe/small-cells-hit-milestone (noting that in the United States, Sprint had deployed one million femtocells as of 2012), *with* CTIA, *Annual Wireless Industry Survey*, *supra* (304,360 traditional cell sites erected by all U.S. wireless carriers as of 2013).

[19] Blaze Hearing Statement, *supra*, at 12. Wireless providers are required to be able to identify the location of small cells, 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) , http://www.3gpp2.org/public_html/specs/S.R0139-0%20v1.0_Femtocell%20Systems%20Overview%20for%20cdma2000%20Wireless%20Communication%20Systems_20110819.pdf.

which they are located can also provide cell connections to passersby, providing highly precise information about location and movement on public streets and sidewalks.[20]

Each call, text message, and data connection to or from a cell phone generates a location record,[21] 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.[22]

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

---

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

[21] The records obtained in this case include cell site information for Gilton's calls, but not for his text messages.

[22] Blaze Hearing Statement, *supra*, at 15.

home, doctor's office, or church with small cells. Likewise, they will not know if a target had a smartphone that may be interacting with the network on a near-continuous basis through data connections, or a traditional feature phone that may communicate less frequently.

A growing body of scholarship illustrates the privacy implications of cell phone location data. For example, 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.[23] Knowing just a few of a person's cell site location points can uniquely identify him or her in the vast majority of cases,[24] can "identify various patterns of life,"[25] or be used to infer demographic information about the cell phone user, including ethnicity and gender.[26] As the New Jersey Supreme Court

---

[23] *See, e.g.* Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Sys. Design & Implementation, at 1–2 (2011), https://www.usenix.org/legacy/events/nsdi11/tech/full_papers/Thiagarajan.pdf?CFID=230550685&CFTOKEN=76524860.

[24] Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Scientific Reports 3 (2013), http://www.nature.com/articles/srep01376.

[25] Neal H. Walfield et al., *A Quantitative Analysis of Cell Tower Trace Data for Understanding Human Mobility and Mobile Networks*, 6th International Workshop on Mobile Entity Localization, Tracking and Analysis (MELT) (2016), http://grothoff.org/christian/melt2016.pdf.

[26] Chris Riederer et al., *"I Don't Have a Photograph, but You Can Have My Footprints."—Revealing the Demographics of Location Data*, Proceedings of the

has explained, "[l]ocation information gleaned from a cell-phone provider can reveal not just where people go—which doctors, religious services, and stores they visit—but also the people and groups they choose to affiliate with and when they actually do so." *State v. Earls*, 70 A.3d 630, 642 (N.J. 2013). "In other words, details about the location of a cell phone can provide an intimate picture of one's daily life." *Id.*

B. Gilton's location information obtained by law enforcement reveals voluminous and private information about his locations and movements.

In this case, using a warrant subsequently found to lack probable cause by the district court, the government requested and received from Gilton's service provider 37 days of historical cell site location information.[27] (ER 1). The records reveal the cell site and sector in which Gilton was located when calls began and ended, thus providing law enforcement with a dense array of data about his locations. Gilton's data include 4,421 separate call records for which CSLI was

---

Ninth International AAAI Conference on Web and Social Media (2015), https://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/view/10576/10474.

[27] Copies of the CSLI records obtained by the government from Gilton's service provider, Sprint, were turned over to the defense in state-court discovery, before the federal indictment was filed. The defense provided these state-court discovery materials to *amici curiae* during preparation of this brief. Although the CSLI data is not part of the record in this case, the government has offered to file it with the Court upon request. Gov't Br. at 14 n.3.

logged, comprising 8,790 cell site location data points.[28] That amounts to an average of 237.6 location points per day, or one location point every six minutes.

This data is particularly revealing of Gilton's location information because of the density of cell sites in urban areas, where he spent much of his time. For example, as of 2012, Sprint, the carrier used by Gilton, operated a total of 66 cell sites within two miles of this Court's San Francisco courthouse, and many more cell sites elsewhere in California.[29] *See* Fig. 1.

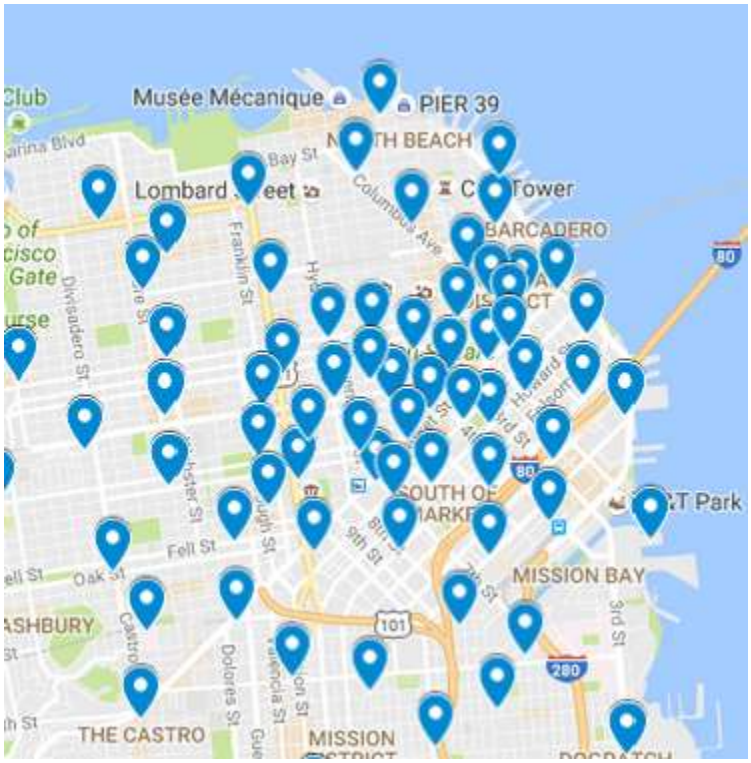

Figure 1: Sprint cell sites in San Francisco, 2012

[28] The records include information about additional calls and text messages for which CSLI was not logged.

[29] The discovery materials include Sprint's lists of its cell sites in greater Los Angeles and in the San Francisco Bay area.

The records obtained by the government reveal many details about Gilton's locations and movements. For example, Gilton's calls show his location in more than 420 separate sectors over the 37 days, and during a typical day his records chart his movements between multiple sectors. On one day, May 21, 2012, he made and received 120 calls for which CSLI was recorded while moving amongst 27 unique cell site sectors. *See* Fig. 2. Even records of individual calls provide information about movement: from May 3 to May 9, 2012, for example, 152 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 Gilton's movements over time.

Figure 2: Cell sites to which Gilton's phone connected at the start (but not the end) of calls on May 21, 2012. Larger circles indicate a larger number of calls connecting with the cell site on that day.

The records also reveal information about particular locations visited. The Sprint cell sites closest to Gilton's home are towers 8 and 217 of switch "LA-BURBANK 2" (aka Repoll # 639). During one five-day period (May 21 through May 25, 2012), Gilton's CSLI records register his phone as being located in the sectors of those towers facing his home 531 times, providing an indication of when

he was in or near his home.[30] The records also allow inferences about where Gilton slept, which could reveal private information about the status of relationships and any infidelities.[31] By sorting the data for the first and last calls of each day, one can infer whether a person slept at home or elsewhere. This information, like that described above, is deeply sensitive and quintessentially private.

II. Obtaining 37 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 States*, 389 U.S. 347, 357 (1967)), the acquisition of Gilton's location records pursuant to a defective search warrant violated his Fourth Amendment rights.

[30] *Amici* obtained Gilton's home address from his counsel, and mapped it onto Sprint's cell tower data.

[31] *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.").

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., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring). 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 constitutionally 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.),[32] 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 shower."). 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

[32] *See also Maynard*, 615 F.3d at 562–63 ("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 . . . .").

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).

Indeed, as the Supreme Court recognized in *United States v. Knotts*, "dragnet type law enforcement practices" that make possible "twenty-four hour surveillance of any citizen of this country" may require application of "different constitutional principles" than have governed more limited forms of surveillance in the past. 460 U.S. 276, 283–84 (1983). The acquisition of longer-term cell phone location records by law enforcement implicates this concern and requires a valid warrant under the Fourth Amendment.

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). "[T]he information the government seeks here is arguably more invasive of an individual's expectation of privacy than the GPS device attached to the defendant's car in *Jones*. . . . [O]ver the course of [many] days an individual

will invariably enter constitutionally protected areas, such as private residences." *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015); *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."), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015).

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*"]. 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; *accord United States v. Davis*, 785 F.3d 498, 540–41 (11th Cir. 2015) (en banc) (Martin, J., dissenting) ("As a government witness testified at trial, 'if you look at the majority of . . . calls over a period of time when somebody wakes up and when somebody goes to sleep, normally it is

fairly simple to decipher where their home tower would be.'"). In this case, Mr. Gilton's cell phone records frequently indicate when he was home. *Supra* Part I.B. 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 small cells 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 federal prosecutions belies the argument that they are imprecise. At trial, prosecutors have used defendants' CSLI to demonstrate, for example, that they were "right where the first robbery was at the exact time of the robbery, the exact sector," Transcript of Jury Trial at 56, *United States v. Carpenter*, No. 12-20218 (E.D. Mich. Dec. 16, 2013), "right in the right sector before the Radio Shack [robbery] in Highland Park," *id.*, "literally right up against the America Gas Station immediately preceding and after [the] robbery occurred," *Davis*, 785 F.3d at 541 (Martin, J., dissenting) (quoting trial transcript) (alteration in original), and "literally . . . right next door to the Walgreen's just before and just after that store was robbed," *id* (alteration in

original).

In this case, law enforcement obtained 37 days of Gilton's location records revealing 8,790 separate location points. It defies logic that this data reveals nothing private about Gilton's life. Quite the opposite: long-term data about a person's locations and movements reveals much information that society recognizes as justifiably private, and its warrantless acquisition violates the Fourth Amendment.

Finally, historical CSLI provides the government with an investigative power it has never had before, a veritable time machine allowing it to reconstruct a person's comings and goings months and years into the past. 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.).

Accordingly, this Court should hold that the acquisition of historical CSLI is a search, and that warrantless requests for it violate the Fourth Amendment. In doing so, the Court should be cognizant of the fact that the precision and volume of CSLI is increasing at a rapid clip. The records in this case date to 2012 and appear

to include CSLI for incoming and outgoing calls. In the intervening years, service providers have increased their capacity to retain CSLI for text messages and data sessions, and to calculate not only the cell site and sector of the phone, but also its distance from the cell tower.[33] Meanwhile, the proliferation of smart phones has resulted in increasing quantities of CSLI generated during data sessions, and the erection of more and more cell sites to accommodate skyrocketing data bandwidth usage.[34] Law enforcement agencies now seek this data from service providers tens of thousands of times each year.[35] This Court should announce a Fourth Amendment rule that adequately protects not only Gilton's CSLI records from 2012, but all cell phone users' CSLI records in 2016 and beyond.

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

The government argues that people have no reasonable expectation of privacy in their cell phone location information because they "assume[] the risk" that their data will be divulged to police if it is "voluntarily conveyed" to a third-party service provider and stored in its business records. Gov't Br. at 29–30. On

---

[33] Silliman, *Technology and Shifting Privacy Expectations*, *supra*.

[34] *Id.*

[35] *See, e.g.*, AT&T, *Transparency Report* 4 (July 2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf (reporting that in a recent one-year period, AT&T received 75,302 requests for cell phone location information).

the contrary, Gilton never voluntarily conveyed his location information to his wireless carrier, and the Supreme Court's business records cases do not extend to the scenario presented here. As several 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.[36] *See, e.g.*, *Third Circuit Opinion*, 620 F.3d at 317–18; *Tracey*, 152 So. 3d at 522–23; *Zanders v. State*, 58 N.E.3d 254, 262–65 (Ind. Ct. App. 2016); *United States v. Alvarez*, No. 14-cr-120, 2016 WL 3163005, at *2–3 (N.D. Cal. June 3, 2016) (Chen, J.); *In re Application for Tel. Info.*, 119 F. Supp. 3d at 1027 (Koh, J.); *United States v. Cooper*, No. 13-

[36] Several courts of appeals have indeed held that the third-party doctrine applies to historical CSLI records. *See* Gov't Br. at 27–28. But the judges of those courts have split deeply over the issue, with the five courts of appeals to consider the Fourth Amendment status of historical CSLI generating 18 separate majority, concurring, and dissenting opinions. *See United States v. Carpenter*, 819 F.3d 880, 883 (6th Cir. 2016) (majority opinion); *id.* at 893 (Stranch, J., concurring); *United States v. Graham*, 824 F.3d 421, 424 (4th Cir. 2016) (en banc) (majority opinion); *id.* at 438 (Wilkinson, J., concurring); *id.* at 441 (Wynn, J., dissenting in part and concurring in the judgment); *United States v. Graham*, 796 F.3d 332, 338 (4th Cir. 2015) (majority opinion), *vacated, reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015); *id.* at 377 (Thacker, J., concurring); *id.* at 378 (Motz, J., dissenting in part and concurring in the judgment); *United States v. Davis*, 785 F.3d 498, 500 (11th Cir. 2015) (en banc) (majority opinion); *id.* at 519 (William Pryor, J., concurring); *id.* at 521 (Jordan, J., concurring); *id.* at 524 (Rosenbaum, J., concurring); *id.* at 533 (Martin, J., dissenting); *United States v. Davis*, 754 F.3d 1205, 1208 (11th Cir. 2014) (unanimous), *vacated, reh'g en banc granted*, 573 F. App'x 925 (11th Cir. 2014); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 602 (5th Cir. 2013) (majority opinion); *id.* at 615 (Dennis, J., dissenting); *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 305 (3d Cir. 2010) (majority opinion); *id.* at 319 (Tashima, J., concurring).

cr-00693-SI-1, 2015 WL 881578, at *8 (N.D. Cal. Mar. 2, 2015) (Illston, J.); *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). That is the correct conclusion, and this Court should follow it here.

Older Supreme Court cases involving the so-called "third-party doctrine" involve distinguishable facts from the type and volume of government surveillance at issue here. Those cases, *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), are "ill suited to the digital age," *Jones*, 132 S. Ct. at 957 (Sotomayor, J.), because they rest on outdated expectations about the "assumption of risk" involved in automatically generating large volumes of sensitive data while using essential technologies.

First, 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. By contrast, in both *Miller* and *Smith*, the Court held that the relevant financial 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. That is not true for CSLI. As the Third Circuit explains:

> 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). Indeed, when a cell phone happens to be roaming on another provider's network, cell phone users "will often not know the identity of the third party to which they are supposedly conveying information." *In re Application for Tel. Info.*, 119 F. Supp. 3d at 1029. And unlike the dialed phone numbers at issue in *Smith*, location information does not appear on a typical user's monthly bill. *See Smith*, 442 U.S. at 742.

Second, even if some people are now aware that their devices produce CSLI, the Supreme Court and this Court have repeatedly recognized that the fact that such information is handled by a third party is not dispositive. *See, e.g.*, *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (diagnostic-test results held by hospital staff); *Bond v. United States*, 529 U.S. 334, 338–39 (2000) (luggage placed in bus overhead bin); *Stoner*, 376 U.S. at 490 (1964) (items stored in rented hotel room). Courts must also weigh an individual's privacy interest in the data itself. *See Miller*, 425 U.S. at 442 ("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."); *Smith*, 442 U.S. at

741-42 (assessing the invasiveness of a pen register and noting its "limited capabilities" such that "'a law enforcement official could not even determine . . . whether a communication existed.'").

This Court has likewise recognized circumstances when individuals retain privacy expectations in information held by third parties. This Court's opinion in *United States v. Golden Valley Electric Association*, 689 F.3d 1108 (9th Cir. 2012), is instructive. There, the Court held that power consumption records held by an electricity company are available to the government without a warrant. *Id.* at 1116. But it recognized that "more inherently personal or private" records might receive greater Fourth Amendment protection, pointing to a Northern District of California decision that highlighted "the personal nature of Google search queries" as an example. *Id.* (citing *Gonzales v. Google, Inc.*, 234 F.R.D. 674, 683–84 (N.D. Cal. 2006)). Similarly, in *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007), this Court found that warrantless surveillance of the internet protocol (IP) addresses held by a third party did not violate the Fourth Amendment, but also expressly clarified that this holding "does not imply that more intrusive techniques or techniques that reveal more content information are also" governed by *Smith* and available without a warrant. *Id.* at 510–11. This Court has also held that "clients of an attorney maintain a legitimate expectation of privacy in their client files" held by the lawyer, *DeMassa v. Nunez*, 770 F.2d 1505, 1506 (9th Cir. 1985), and that

patients of an abortion clinic have a reasonable expectation of privacy in their medical records held by the provider, *Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 550 (9th Cir. 2004). Recently, in *In re Grand Jury Subpoena, JK-15-029* (*United States v. Kitzhaber*), 828 F.3d 1083, 1086 (9th Cir. 2016), this Court recognized that a government employee has a reasonable expectation of privacy in copies of personal emails stored on a government server. *Accord United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding that people have a reasonable expectation of privacy in emails stored on a service provider's servers). These cases confirm that the privacy interest in records held by a third party is relevant to whether the Fourth Amendment's protections apply.

Here, the privacy interest in long-term CSLI is fundamentally different from the handful of dialed telephone numbers in *Smith* or the deposit slips and canceled checks in *Miller*. Comparing these records to modern communications metadata is like "saying a ride on horseback is materially indistinguishable from a flight to the moon." *See Riley*, 134 S. Ct. at 2488; *see also United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (en banc) (distinguishing the search of a laptop from the search of hand luggage) ("The point is technology matters."). The sheer volume and pervasiveness of long-term CSLI can reveal a wealth of information about a person's daily life and most private affairs, including expressive and associational activities that have traditionally received heightened Fourth

Amendment scrutiny. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 565 (1978) (recognizing that courts must "apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search."). It strains credulity to conclude that people "voluntarily" convey this information to service providers—let alone "assume the risk" that law enforcement will access it—simply by carrying a cell phone.

In fact, recent studies show that Americans expect their location information to remain private. In 2014, the Pew Research Center reported that 82% of Americans consider the details of their physical location over time to be sensitive information—with more people deeming it as sensitive than their relationship history, religious or political views, or the content of their text messages.[37] In 2012, another study found that cell phone owners take steps to protect their personal information and mobile data, including turning off location tracking on their phones, which disables location tracking for certain apps but does not prevent the service provider from logging CSLI.[38] A 2013 survey conducted on behalf of

[37] Mary Madden et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center 34, 36–37 (Nov. 12, 2014) *available at* http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (50% of respondents believed location information was "very sensitive.").

[38] Jan Lauren Boyles et al., *Privacy and Data Management on Mobile Devices*, Pew Research Internet & American Life Project (Sept. 5, 2012) *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf; Kathryn Zickuhr, *Location-Based Services*, Pew Research Internet and American Life Project 3

Internet company TRUSTe found 69% of American smartphone users were concerned about being tracked.[39] And a 2009 Carnegie Mellon survey of perceptions about location-sharing technologies showed that, on average, participants believed the risks of location-sharing technologies outweighed the benefits and were "extremely concerned" about controlling access to their location information.[40]

Finally, it is a Fourth Amendment fiction that individuals have a legitimate choice about whether to convey CSLI to service providers. Generating location information is an inescapable consequence of using a cell phone. There is no alternative—no option to mask the metadata, no option to close the proverbial phone booth door.[41] *See Katz*, 389 U.S. at 352. Indeed, as some courts have

---

(Sept. 12, 2013), http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Location-based%20services%202013.pdf (46% of teenagers turned location services off).

[39] Dave Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTe Blog (Sept. 5, 2013), http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size/.

[40] Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University 11–13 (Feb. 2010), *available at* http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

[41] 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. *In re Application for Tel. Info.*, 119 F. Supp. 3d at 1025.

suggested, the only way to avoid producing an unauthorized autobiography is to stop using cell phones. *See, e.g.*, *Graham*, 824 F.3d at 428 (en banc); *Carpenter*, 819 F.3d at 888. But when a phone can be considered a "feature of human anatomy," owning and carrying one is hardly a choice at all. *Riley*, 134 S. Ct. at 2484. As the Supreme Court has repeatedly recognized, the privacy of such communications is essential to the exercise of First Amendment freedoms. *See City of Ontario v. Quon*, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."); *Riley*, 134 S. Ct. at 2484; *see also Cooper*, 2015 WL 881578, at *8 (cell phones are "ubiquitous, and for many, an indispensible gizmo to navigate the social, economic, cultural, and professional realms of modern society.").

Long-term CSLI is not a simple business record voluntarily conveyed by cell phone users. It is window back in time, a transcript of a person's movements over weeks, months, and years—nothing like what the Supreme Court considered in *Miller and Smith*. On the contrary, the Supreme Court has cautioned against allowing new technology 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."). This Court should take that

admonition seriously and find that 37 days' worth of location tracking falls outside of the ambit of the Fourth Amendment, just as 28 days was too much for the Justices in *Jones*. 132 S. Ct. at 955 (Sotomayor, J.); *id.* at 963–64 (Alito, J.). As the Florida Supreme Court has 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.

CONCLUSION

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

Respectfully Submitted,

Dated: November 3, 2016

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

Linda Lye
American Civil Liberties Union Foundation of Northern California
39 Drumm Street, 2nd Floor
San Francisco, California
(415) 621-2493

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
1401 K St., NW
Suite 200
Washington, DC 20005
(202) 637-9800
gnojeim@cdt.org

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

David M. Porter
National Association of Criminal
Defense Lawyers
Co-chair, NACDL Amicus Curiae
Committee
801 I Street, 3rd Floor
Sacramento, California 95814
(916) 498-5700

Kevin S. Bankston
Ross Schulman
New America's Open Technology
Institute

740 15th St., N.W., Suite 900
Washington, DC 20005
(202) 986-2700

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rules of Appellate Procedure 29(d) and 32(a) because it contains 6,982 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).
2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman.

/s/ Nathan Freed Wessler

Nathan Freed Wessler

November 3, 2016

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 3rd day of November, 2016, the foregoing Amici Curiae Brief for the American Civil Liberties Union, the American Civil Liberties Union of Northern California, the Brennan Center for Justice, the Center for Democracy & Technology, the Electronic Frontier Foundation, the National Association of Criminal Defense Lawyers, and New America's Open Technology Institute 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