


No. _____

IN THE
Supreme Court of the United States



TIMOTHY IVORY CARPENTER,
Petitioner,

—v.—

UNITED STATES OF AMERICA,
Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES
COURT OF APPEALS FOR THE SIXTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES
UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Steven R. Shapiro
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226

QUESTION PRESENTED

In this case, as in thousands of cases each year, the government sought and obtained the historical cell phone location data of a private individual pursuant to a disclosure order under the Stored Communications Act (SCA) rather than by securing a warrant. Under the SCA, a disclosure order does not require a finding of probable cause. Instead, the SCA authorizes the issuance of a disclosure order whenever the government “offers specific and articulable facts showing that there are reasonable grounds to believe” that the records sought “are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d).

As a result, the district court never made a probable cause finding before ordering Petitioner’s service provider to disclose months’ worth of Petitioner’s cell phone location records. A divided panel of the Sixth Circuit held that there is no reasonable expectation of privacy in these location records, relying in large part on four-decade-old decisions of this Court.

The Question Presented is:

Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment.

PARTIES TO THE PROCEEDINGS

In addition to the parties named in the caption, Timothy Michael Sanders was a defendant-appellant below, and was represented by separate counsel.

TABLE OF CONTENTS

QUESTION PRESENTED	i
PARTIES TO THE PROCEEDINGS	ii
TABLE OF AUTHORITIES	vi
PETITION FOR A WRIT OF CERTIORARI.....	1
OPINIONS BELOW	1
JURISDICTION.....	1
RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS	1
STATEMENT OF THE CASE.....	3
REASONS FOR GRANTING THE WRIT	10
I. THIS CASE PRESENTS AN IMPORTANT AND RECURRING QUESTION ON THE SCOPE OF CONSTITUTIONAL PRIVACY RIGHTS IN THE DIGITAL AGE.....	10
A. The Lower Courts Have Expressly and Repeatedly Sought This Court’s Guidance in Addressing the Question Presented. ...	10
B. This Court’s Recent Decisions Have Properly Recognized a Need to Reexamine Traditional Understandings of Privacy in the Digital Age.....	16
C. The Volume and Frequency of Warrantless Law Enforcement Requests for CSLI Highlights the Importance of the Question Presented.	18

II. FEDERAL COURTS OF APPEALS AND STATE HIGH COURTS ARE DIVIDED.	21
A. The Circuits Are Split Over Whether the Third-Party Doctrine Eliminates People’s Reasonable Expectation of Privacy in Their Historical CSLI.	21
B. The Circuits Are Split Over Whether There is a Reasonable Expectation of Privacy in Longer-Term Location Information Collected by Electronic Means.	24
III. THE SIXTH CIRCUIT ERRED IN HOLDING THAT THE CONDUCT HERE WAS NOT A SEARCH.....	26
A. The Sixth Circuit Erred in Holding That There Is No Reasonable Expectation of Privacy in Historical CSLI.	26
B. The Sixth Circuit Erred In Deferring to Congress’s 30-Year-Old Legislative Scheme.	32
CONCLUSION.....	35
APPENDIX.....	1a
Opinion, United States Court of Appeals for the Sixth Circuit (April 13, 2016)	1a
Order, United States Court of Appeals for the Sixth Circuit (June 29, 2016)	33a
Opinion & Order, United States District Court, Eastern District Of Michigan, Southern Division (Dec. 6, 2013)	34a

Application, United States District Court, Eastern District Of Michigan, Southern Division (May 2, 2011)..... 49a

Order, United States District Court, Eastern District of Michigan, Southern Division (May 2, 2011)..... 56a

Application, United States District Court, Eastern District of Michigan, Southern Division (June 7, 2011)..... 62a

Order, United States District Court, Eastern District of Michigan, Southern Division (June 7, 2011)..... 69a

Government Trial Exhibit 57, Federal Bureau Of Investigation Cellular Analysis (Nov. 5, 2013)... 74a

TABLE OF AUTHORITIES

CASES

<i>Bond v. United States</i> , 529 U.S. 334 (2000)	27
<i>Chapman v. United States</i> , 365 U.S. 610 (1961)	27
<i>Commonwealth v. Augustine</i> , 4 N.E.3d 846 (Mass. 2014)	23
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001) .	27
<i>Florida v. Jardines</i> , 133 S. Ct. 1409 (2013)	26
<i>In re Application for Tel. Info. Needed for a Criminal Investigation</i> , 119 F. Supp. 3d 1011 (N.D. Cal. 2015), <i>appeal dismissed</i> , No. 15-16760 (9th Cir. Feb. 5, 2016)	29
<i>In re Application of the U.S. for Historical Cell Site Data</i> , 724 F.3d 600 (5th Cir. 2013)	14, 22, 34
<i>In re Application of U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to Gov't</i> , 620 F.3d 304 (3d Cir. 2010)	14, 22, 23, 28
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	<i>passim</i>
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	17, 26, 28, 30
<i>Minnesota v. Olson</i> , 495 U.S. 91 (1990)	27
<i>New York v. Belton</i> , 453 U.S. 454 (1981)	16
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	<i>passim</i>
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	<i>passim</i>
<i>State v. Earls</i> , 70 A.3d 630 (N.J. 2013)	24
<i>Stoner v. California</i> , 376 U.S. 483 (1964)	27

<i>Tracey v. State</i> , 152 So. 3d 504 (Fla. 2014).....	24, 32
<i>United States v. Davis</i> , 754 F.3d 1205 (11th Cir. 2014), <i>rev'd en banc</i> , 785 F.3d 498 (11th Cir. 2015)	14, 29
<i>United States v. Davis</i> , 785 F.3d 498 (11th Cir. 2015), <i>cert. denied</i> , 136 S. Ct. 479 (2015)	<i>passim</i>
<i>United States v. Garcia</i> , 474 F.3d 994 (7th Cir. 2007)	25
<i>United States v. Graham</i> , 796 F.3d 332 (4th Cir. 2015), <i>rev'd en banc</i> , 824 F.3d 421 (4th Cir. 2016)	14
<i>United States v. Graham</i> , 824 F.3d 421 (4th Cir. 2016)	<i>passim</i>
<i>United States v. Guerrero</i> , 768 F.3d 351 (5th Cir. 2014)	22
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984).....	27
<i>United States v. Jones</i> , 132 S. Ct. 945 (2012) ...	<i>passim</i>
<i>United States v. Karo</i> , 468 U.S. 705 (1984)	29
<i>United States v. Marquez</i> , 605 F.3d 604 (8th Cir. 2010)	25
<i>United States v. Maynard</i> , 615 F.3d 544 (D.C. Cir. 2010)	24, 25
<i>United States v. Miller</i> , 425 U.S. 435 (1976) ...	<i>passim</i>
<i>United States v. Pineda-Moreno</i> , 617 F.3d 1120 (9th Cir. 2010)	20, 25
<i>United States v. Skinner</i> , 690 F.3d 772 (6th Cir. 2012)	8
<i>United States v. Knotts</i> , 460 U.S. 276 (1983).....	20

<i>Zanders v. State</i> , No. 15A01–1509–CR–1519, __ N.E.3d __, 2016 WL 4140998 (Ind. Ct. App. Aug. 4, 2016), <i>pet. to transfer jurisdiction to Indiana</i> <i>Supreme Court filed</i> (Sept. 6, 2016).....	14, 23
--	--------

CONSTITUTION & STATUTES

U.S. Const. amend. IV	<i>passim</i>
Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 207, 108 Stat. 4279 (1994)	33
Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848	33
Hobbs Act, 18 U.S.C. § 1951(a)	9
Stored Communications Act, 18 U.S.C. § 2703 <i>et seq.</i>	<i>passim</i>
18 U.S.C. § 2703(c)(1)(A)	34
18 U.S.C. § 2703(d)	i, 3, 22
18 U.S.C. § 924(c).....	9
28 U.S.C. § 1254(1)	1
725 Ill. Comp. Stat. 168/10	24
Colo. Rev. Stat. § 16-3-303.5(2)	23
Ind. Code 35-33-5-12.....	24
Md. Code Ann. Crim. Proc. § 1-203.1(b).....	24
Me. Rev. Stat. tit. 16, § 648	23
Minn. Stat. §§ 626A.28(3)(d), 626A.42(2).....	23
Mont. Code Ann. § 46-5-110(1)(a)	23
N.H. Rev. Stat. Ann. § 644-A:2.....	23
Utah Code Ann. § 77-23c-102(1)(a)	23

Va. Code Ann. § 19.2-70.3(C).....	24
Vt. Stat. Ann. tit. 13, § 8102(b)	23

OTHER AUTHORITIES

American Civil Liberties Union, Cell Phone Location Tracking Public Records Request (Mar. 25, 2013)	20
Andrea Meyer, <i>30th Anniversary of the First Commercial Cell Phone Call</i> , Verizon (Oct. 11, 2013)	33, 34
Arvind Thiagarajan et al., <i>Accurate, Low-Energy Trajectory Mapping for Mobile Devices</i> , 8 USENIX Conf. on Networked Syss. Design & Implementation 20 (2011).....	31
AT&T, <i>Transparency Report</i> (2015).....	19
<i>Background on CTIA’s Wireless Industry Survey</i> , CTIA-The Wireless Association (2014).....	33
CTIA – The Wireless Association, <i>Annual Wireless Industry Survey</i> (2014).....	7, 18, 33
Daniel Solove, <i>Conceptualizing Privacy</i> , 90 Calif. L. Rev. 1087 (2002).....	15
Pew Research Ctr., <i>Public Perceptions of Privacy and Security in the Post-Snowden Era</i> (Nov. 12, 2014).....	32
Sherry F. Colb, <i>What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy</i> , 55 Stan. L. Rev. 119 (2002).....	15

Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, <i>Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January–June 2014</i> (Dec. 2014)	18
T-Mobile, <i>Transparency Report for 2013 & 2014 (2015)</i>	19
Will Baude, <i>Further Thoughts on the Precedential Status of Decisions Affirmed on Alternate Grounds, The Volokh Conspiracy</i> (Dec. 3, 2013, 7:27 PM), <a href="http://volokh.com/2013/12/03/thoughts-
precedential-status-decisions-affirmed-alternate-
grounds/">http://volokh.com/2013/12/03/thoughts- precedential-status-decisions-affirmed-alternate- grounds/	25

PETITION FOR A WRIT OF CERTIORARI

Petitioner Timothy Carpenter respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Sixth Circuit.

OPINIONS BELOW

The opinion of the Sixth Circuit (Pet. App. 1a–32a) is reported at 819 F.3d 880. The district court opinion (Pet. App. 34a–48a) is unpublished, but is available at 2013 WL 6385838.

JURISDICTION

The Sixth Circuit issued its opinion on April 13, 2016, and denied rehearing en banc on June 29, 2016. (Pet. App. 33a). This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment to the U.S. Constitution provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Stored Communications Act, 18 U.S.C. § 2703, provides in relevant part:

(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; [or]

(B) obtains a court order for such disclosure under subsection (d) of this section; * * *

(d) Requirements for court order.-- A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other

information sought, are relevant and material to an ongoing criminal investigation. * * *

STATEMENT OF THE CASE

This case presents the pressing question of whether the Fourth Amendment protects against the government's warrantless acquisition of cell phone records revealing an individual's location and movements over extended periods of time.

1. During the course of an investigation into a series of armed robberies that occurred in southeastern Michigan and northwestern Ohio in 2010 and 2011, an Assistant United States Attorney submitted to different magistrate judges three applications for orders to access more than five months of historical cell phone location records for Petitioner Timothy Carpenter and several other suspects. Pet. App. 3a, 49a–55a, 62a–68a. The applications, which were unsworn, did not seek warrants based on probable cause, but rather orders under the Stored Communications Act, 18 U.S.C. § 2703(d). Such an order may issue when the government “offers specific and articulable facts showing that there are reasonable grounds to believe that” the records sought “are relevant and material to an ongoing criminal investigation.” *Id.*

The applications sought “[a]ll subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target telephones from December 1, 2010 to present[,]” as well as “cell site information for the target telephones at call origination and at call termination

for incoming and outgoing calls[.]” Pet. App. 4a (alterations in original); *see also id.* at 52a. The applications stated that “a cooperating defendant was interviewed about his involvement in [several] armed robberies and admitted he had a role in eight different robberies that started in December of 2010 and lasted through March of 2011 at Radio Shack and T-Mobile stores in Michigan and Ohio.” Pet. App. 53a. The applications further asserted that “the requested telecommunications records should yield information that is relevant and material to corroborate surveillance information and may identify potential witnesses and/or targets. The requested information will . . . provide evidence that . . . Timothy Carpenter and other known and unknown individuals are violating provisions of Title 18, United States Code, §1951.” Pet. App. 54a. Rather than restricting the request to only the days on which the robberies occurred, however, the primary application at issue here, which was submitted on May 2, 2011, sought records “from December 1, 2010 to present.” Pet. App. 52a. That constituted a request for 152 days of data.

Orders granting the applications were issued on May 2 and June 7, 2011. Pet. App. 56a–61a, 69a–73a. The May 2 order directed MetroPCS, Carpenter’s cellular service provider, to “provide the locations of cell/site sector (physical addresses) for the target telephones at call origination and at call termination for incoming and outgoing calls” from “December 1, 2010 to present.” Pet. App. 59a–60a. MetroPCS complied, providing 186 pages of

Carpenter's cell phone records to the government.¹ Those records show each of Carpenter's incoming and outgoing calls over the course of 127 days,² along with the cell tower ("cell site") and directional sector of the tower that Carpenter's phone connected to at the start and end of most of the calls.³ Pet. App. 5a–7a.

A separate order, issued on June 7, 2011, directed Sprint to produce cell site location information for Carpenter's phone while it was "roaming on Sprint's cellular tower network" from March 1 to March 7, 2011. Pet. App. 72a. "Metro PCS does not have coverage in the Warren, Ohio area," where one of the charged robberies took place, and

¹ A sample page from Carpenter's records was entered into evidence at trial. Defendant's Trial Ex. 3. The full records were provided by the government to the defense in pre-trial discovery and were discussed by a prosecution's witness at trial, Trial Tr. 46, Dec. 13, 2013, ECF No. 332, but were not made part of the record before the district court. They were filed as an appendix to the Amicus Brief of the American Civil Liberties Union, et al., at the Sixth Circuit. See Doc. No. 33-1 The parties stipulated at trial that the cell site location records from "Metro PCS and Sprint utilized by [government witness] FBI Special Agent Christopher Hess to formulate his analysis and opinion are authentic and accurate business records of these companies." Gov't Trial Ex. 58; Trial Tr. 47, Dec. 13, 2013, ECF No. 332.

² Although the government's application and resulting court order sought 152 days of records (December 1, 2010 through May 2, 2011), MetroPCS produced 127 days of records (December 1, 2010 through April 6, 2011).

³ Cell sites, which are the transmitting towers through which cell phones communicate with the telephone network, consist of antennas facing different directions that cover distinct wedge-shaped "sectors."

has a “roaming agreement . . . with Sprint, which does cover that area.” Trial Tr. 59, Dec. 13, 2013, ECF No. 332.⁴ Therefore, Sprint, not MetroPCS, possessed Carpenter’s cell site location information for calls made and received while he was in Ohio. Sprint produced two pages of call detail records with cell site location information for March 3 and 4, 2011.

MetroPCS and Sprint also produced lists of their cell sites in southern Michigan and northwestern Ohio, respectively, providing the longitude, latitude, and physical address of each cell site, along with the directional orientation of each sector antenna. *See id.* at 74. By cross-referencing the information in Carpenter’s call detail records with these cell-site lists, the government could identify the area in which Carpenter’s phone was located and could thereby deduce Carpenter’s location and movements at multiple points each day.

2. The precision of a cell phone user’s location reflected in cell site location information (“CSLI”) records depends on the size of the cell site sectors in the area. Most cell sites consist of multiple directional antennas that divide the cell site into “sectors.” Pet. App. 5a. The coverage area of cell site sectors is smaller in areas with greater density of cell towers, with urban areas having the greatest density and thus the smallest coverage areas. *Id.*; *see also* Pet. App. 88a (Gov’t Trial Ex. 57, at 13) (providing maps of MetroPCS and Sprint cell sites).

⁴ As explained at trial, “[i]n a roaming situation, if [a service provider] doesn’t have coverage in a particular area of the country, they would have an agreement with another company to be able to utilize their infrastructure.” *Id.* at 39–40.

The density of cell sites continues to increase as data usage from smartphones grows. Because each cell site can carry only a fixed volume of data required for text messages, emails, web browsing, streaming video, and other uses, as smartphone data usage increases carriers must erect additional cell sites, each covering smaller geographic areas. See CTIA – The Wireless Association, *Annual Wireless Industry Survey* (2016)⁵ (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). This means that in urban and dense suburban areas like Detroit, many sectors cover small geographic areas and therefore can provide relatively precise information about the location of a phone. Pet. App. 5a.

Although in this case MetroPCS provided only information identifying Carpenter’s cell site and sector at the start and end of his calls, service providers increasingly retain more granular historical location data, including for text messages and data connections. *United States v. Davis*, 785 F.3d 498, 542 (11th Cir. 2015) (en banc) (Martin, J., dissenting). Location precision is also increasing as service providers deploy millions of “small cells,” “which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home.” *United States v. Graham*, 824 F.3d 421, 448 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in

⁵ Available at <http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey>.

part and concurring in the judgment) (citation omitted).

3. Before trial, Carpenter joined his codefendant's motion to suppress the CSLI records on the basis that their acquisition pursuant to the "reasonable grounds standard" in the Stored Communications Act . . . is unconstitutional." Pet. App. 36a; *see also id.* at 4a. Relying on *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), a case holding that no warrant is required for short-term real-time tracking of a suspect's cell phone, the district court denied the motion on the basis that acquisition of the cell-site records was not a Fourth Amendment search. Pet. App. 38a–39a.

At trial, the government introduced information about Carpenter's CSLI records and relied on them to establish Carpenter's location on the days of the charged robberies. FBI Special Agent Christopher Hess testified that Carpenter's CSLI records placed him near the sites of four of the robberies. Pet. App. 5a–6a. Hess also produced maps showing the location of Carpenter's phone relative to the locations of the robberies, which the government introduced into evidence. Pet. App. 6a; *Id.* at 86a–89a (Gov't Trial Ex. 57). The government relied on the records to show Carpenter's proximity to "the robberies around the time the robberies happened." Pet. App. 6a. The prosecutor argued to the jury, for example, that Mr. Carpenter was "right where the first robbery was at the exact time of the robbery, the exact sector," Trial Tr. 56, Dec. 16, 2013, ECF No. 333, and that he was "right in the right sector before the Radio Shack in Highland Park," *id.* *See also* Trial

Tr. 49–62, Dec. 13, 2013, ECF No. 332 (testimony of Special Agent Hess).

The jury convicted Carpenter of six robberies in violation of the Hobbs Act, 18 U.S.C. § 1951(a), and five separate violations of 18 U.S.C. § 924(c) for using or carrying a firearm in connection with a federal crime of violence and aiding and abetting. All but the first of the § 924(c) convictions carried mandatory consecutive minimum sentences of 25 years each. As a result, the court sentenced Carpenter to nearly 116 years' imprisonment (1,395 months).

5. On appeal, a divided three-judge panel of the Sixth Circuit held that no search occurred under the Fourth Amendment because Carpenter had no reasonable expectation of privacy in cell phone location records held by his service provider. Pet. App. 17a. Writing for the majority, Judge Kethledge concluded that people do not have a reasonable expectation of privacy in CSLI because it is a business record of the service provider that reveals routing information rather than the contents of communications. Pet. App. 10a–11a. Judge Kethledge relied in part on this Court's 1979 decision in *Smith v. Maryland*, 442 U.S. 735 (1979), reasoning that like the dialed phone numbers conveyed to the phone company in *Smith*, people knowingly expose their location information to their service provider and therefore lack an expectation of privacy in it. Pet. App. 11a–12a.

Judge Stranch disagreed. Concurring in the judgment only, she explained that “the sheer quantity of sensitive information procured without a warrant in this case raises Fourth Amendment

concerns of the type the Supreme Court . . . acknowledged in *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).” Pet. App. 24a. “I do not think that treating the CSLI obtained as a ‘business record’ and applying that test addresses our circuit’s stated concern regarding long-term, comprehensive tracking of an individual’s location without a warrant.” *Id.* at 29a. Judge Stranch concluded, however, that suppression was not warranted under the good-faith exception to the exclusionary rule, a question that the majority did not address. *Id.* at 29a–31a. On that alternative basis, she concurred in the judgment.

REASONS FOR GRANTING THE WRIT

I. THIS CASE PRESENTS AN IMPORTANT AND RECURRING QUESTION ON THE SCOPE OF CONSTITUTIONAL PRIVACY RIGHTS IN THE DIGITAL AGE.

A. The Lower Courts Have Expressly and Repeatedly Sought This Court’s Guidance in Addressing the Question Presented.

The question at the center of this case—whether there is a reasonable expectation of privacy under the Fourth Amendment in a person’s cell site location information held by their cellular service provider—requires definitive resolution by this Court. Numerous lower court judges addressing the issue have explained that they feel bound by this Court’s third-party–doctrine cases from the 1970s, but that they are discomfited by the result they believe those cases require them to reach. Only this Court can provide the guidance they seek about

whether and how a doctrine developed long before the digital age applies to the voluminous and sensitive digital records at issue here. More specifically, only this Court can determine whether *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), render the Fourth Amendment irrelevant when the government seeks detailed records from a cell phone provider cataloging the location and movements of a cell phone user over many months.

In *Smith*, this Court ruled that the short-term use of a pen register to capture the telephone numbers a person dials is 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. The Court also assessed the degree of invasiveness of the surveillance to determine whether the user had a reasonable expectation of privacy. The Court noted the “pen register’s limited capabilities,” *id.* at 742, explaining that “a law enforcement official could not even determine from the use of a pen register whether a communication existed.” *Id.* at 741 (citation omitted). Similarly, in *Miller*, the Court concluded that bank customers do not have any Fourth Amendment interest in their bank records because all the information in those records has been voluntarily conveyed to the bank. 425 U.S. 435, 440–42 (1976). The principle sometimes discerned from these cases, that certain records or information shared with third parties deserve no Fourth Amendment protection, is known as the “third-party doctrine.”

Lacking further guidance from this Court, lower courts have been struggling to apply the pre-digital holdings in *Smith* and *Miller* to newer forms of pervasive digital data.

In *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc), *cert. denied*, 136 S. Ct. 479 (2015), for example, a majority of the en banc Eleventh Circuit held that this Court’s decisions in *Smith* and *Miller* require the conclusion that there is no Fourth Amendment protection for CSLI records. But while the Eleventh Circuit believed it “remains bound by *Smith* and *Miller*,” 785 F.3d at 514, two separate concurrences called on this Court to clarify the scope of those decisions, evincing discomfort with their application to the records at issue. As Judge Rosenbaum wrote:

In our time, unless a person is willing to live “off the grid,” it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling. . . . Since we are not the Supreme Court and the third-party doctrine continues to exist and to be good law at this time, though, we must apply the third-party doctrine where appropriate.

Id. at 525 (Rosenbaum, J., concurring); *see also id.* at 519, 521 (William Pryor, J., concurring) (“[W]e must leave to the Supreme Court the task of developing

exceptions to the rules it has required us to apply. . . . As judges of an inferior court, we have no business in anticipating future decisions of the Supreme Court. If the third-party doctrine results in an unacceptable ‘slippery slope,’ the Supreme Court can tell us as much. That is, if ‘the Supreme Court has given reasons to doubt the rule’s breadth,’ it alone must decide the exceptions to its rule.” (citations omitted)).

Likewise, the en banc majority of the Fourth Circuit wrote that “[t]he Supreme Court may in the future limit, or even eliminate, the third-party doctrine. . . . But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case.” *United States v. Graham*, 824 F.3d 421, 425 (4th Cir. 2016) (en banc). And in this case, Judge Stranch discussed her “concern[] about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled,” concluding that there is a “need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances.” Pet. App. 29a (Stranch, J., concurring).

All told, the five courts of appeals to consider the Fourth Amendment status of historical CSLI have generated 18 separate majority, concurring, and dissenting opinions, highlighting the need for this Court to act. *See* Pet. App. 1a (majority opinion); *id.* at 24a (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) [*Fifth Circuit CSLI Opinion*] (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) [*Third Circuit CSLI Opinion*] (majority opinion); *id.* at 319 (Tashima, J., concurring).

As reflected in these 18 opinions attempting to grapple with the same basic issue, lower courts are divided over how to apply the third-party doctrine to CSLI records. *Compare Graham*, 824 F.3d at 424–25 (no expectation of privacy in CSLI under *Smith*), *Davis*, 785 F.3d at 511–13 (same), and *Fifth Circuit CSLI Opinion*, 724 F.3d at 612–13 (same), with *Third Circuit CSLI Opinion*, 620 F.3d at 317 (distinguishing *Smith* and holding that cell phone users may retain a reasonable expectation of privacy in CSLI); *Zanders v. State*, No. 15A01–1509–CR–1519, __ N.E.3d __, 2016 WL 4140998, at *8–10 (Ind. Ct. App. Aug. 4, 2016) (distinguishing *Smith* and *Miller* and holding that “the third-party doctrine

does not dictate the outcome of this case”), *pet. to transfer jurisdiction to Indiana Supreme Court* filed (Sept. 6, 2016).

This struggle to define the scope of Fourth Amendment protection for newer forms of sensitive digital data reflects, at least in part, scholarly criticism of the expansive application of the third-party doctrine beyond the kinds of records at issue in *Smith* and *Miller*. See, e.g., Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 *Stan. L. Rev.* 119 (2002); Daniel J. Solove, *Conceptualizing Privacy*, 90 *Calif. L. Rev.* 1087, 1151–52 (2002). These scholars have joined the lower courts in calling on this Court to ensure that the Fourth Amendment keeps pace with the rapid advance of technology.

In sum, there is a substantial question of how the protections of the Fourth Amendment should apply to sensitive and private data in the hands of trusted third parties. As Justice Sotomayor noted in *United States v. Jones*,

it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.

132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

It is not necessary in this case to reassess the continued validity of the third-party doctrine in every possible context. But it is critically important to clarify the scope of analog-age precedents to digital surveillance techniques. Without guidance from this Court, a cell phone user “cannot know the scope of his constitutional protection, nor can a policeman know the scope of his authority.” *New York v. Belton*, 453 U.S. 454, 459–60 (1981). As law enforcement seeks ever greater quantities of location data and other sensitive digital records, the need for this Court to speak grows daily more urgent.

B. This Court’s Recent Decisions Have Properly Recognized a Need to Reexamine Traditional Understandings of Privacy in the Digital Age.

Twice in recent terms this Court has confronted crucial questions regarding the application of the Fourth Amendment in the digital age. *See Riley v. California*, 134 S. Ct. 2473 (2014) (warrant required for search of cell phone seized incident to lawful arrest); *United States v. Jones*, 132 S. Ct. 945 (2012) (tracking car with GPS device is a Fourth Amendment search). This case presents an important next step in the ongoing effort to reconcile enduring Fourth Amendment principles with the reality of a new digital world.

In *United States v. Jones*, this Court addressed the pervasive location monitoring made possible by GPS tracking technology surreptitiously and warrantlessly attached to a vehicle. All members of the Court agreed that attaching a GPS device to a vehicle and tracking its movements constitutes a

search under the Fourth Amendment. In so holding, the Court made clear that the government’s use of novel digital surveillance technologies not in existence at the framing of the Fourth Amendment does not escape the Fourth Amendment’s reach. 132 S. Ct. at 950–51 (“[W]e must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001))); *id.* at 963–64 (Alito, J., concurring in the judgment) (“[S]ociety’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.”).

In *Riley v. California*, the Court addressed Americans’ privacy rights in the contents of their cell phones, unanimously holding that warrantless search of the contents of a cell phone incident to a lawful arrest violates the Fourth Amendment. In so doing, the Court rejected the government’s inapt analogy to other physical objects that have historically been subject to warrantless search incident to an arrest. 134 S. Ct. at 2489 (“Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person.”).

Monitoring an individual’s location and movements over an extended period of time by collecting and analyzing cell phone records can and frequently will expose extraordinarily sensitive details of a person’s life including, potentially, “a wealth of detail about . . . familial, political, professional, religious, and sexual associations.”

Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring). Without disputing that premise, the court of appeals nonetheless held that this voluminous documentation of a person’s movements in public *and* private spaces is unprotected by the Fourth Amendment by analogizing to the kinds of limited analog data at issue in *Smith* and *Miller*. Pet. App. 11a–14a. As this Court recently cautioned, however, unexamined reliance on “pre-digital analogue[s]” risks causing “a significant diminution of privacy.” *Riley*, 134 S.Ct. at 2493. Accordingly, “any extension of . . . reasoning [from decisions concerning analog searches] to digital data has to rest on its own bottom.” *Id.* at 2489. Only this Court can make that ultimate constitutional judgment.

C. The Volume and Frequency of Warrantless Law Enforcement Requests for CSLI Highlights the Importance of the Question Presented.

“[M]ore than 90% of American adults . . . own a cell phone.” *Riley*, 134 S. Ct. at 2490. As of December 2015, there were more than 377 million wireless subscriber accounts in the United States.⁶ Forty-four percent of U.S. households have *only* cell phones.⁷ When “nearly three-quarters of smart phone

⁶ CTIA – The Wireless Association, *Annual Wireless Industry Survey* (2016), <http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey>.

⁷ Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January–June 2014* 1 (Dec. 2014), <http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201412.pdf>.

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,” *Riley*, 134 S. Ct. at 2490, the privacy implications of warrantless law enforcement access to cell phone location data are difficult to overstate.

This is not an isolated or occasional concern. Law enforcement is requesting staggering volumes of CSLI from service providers. From July 2015 to June 2016, for example, AT&T received 75,302 requests for cell phone location information.⁸ Verizon received approximately 18,935 requests for cell phone location data in just the first half of 2016.⁹

The government often obtains large volumes of CSLI pursuant to such requests. In this case the government requested five months’ and obtained nearly four months’ (127 days’) worth of Carpenter’s location data comprising thousands of location data points. A request for months of data is no aberration: according to T-Mobile, which now owns Carpenter’s service provider, MetroPCS, the average law enforcement request “asks for approximately fifty-five days of records.”¹⁰ Other recent and pending cases involve comparable or even greater quantities

⁸ AT&T, *Transparency Report*, at 4 (2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf.

⁹ Verizon, *Transparency Report 1H 2016*, at 5 (2016), <https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report-US-1H-2016.pdf>.

¹⁰ T-Mobile, *Transparency Report for 2013 & 2014*, at 5 (2015), <http://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf>.

of sensitive location information obtained without a warrant. In one case, the government obtained 221 days (more than seven months) of cell site location information, revealing 29,659 location points for one defendant. *See Graham*, 824 F.3d at 446–47 (Wynn, J., dissenting in part and concurring in the judgment).

In *Jones*, Justice Alito recognized that of the “many new devices that permit the monitoring of a person’s movements,” cell phones are “[p]erhaps most significant.” 132 S. Ct. at 963 (Alito, J., concurring in the judgment). Yet most law enforcement agencies are obtaining these large quantities of historical CSLI without a probable cause warrant. *See American Civil Liberties Union, Cell Phone Location Tracking Public Records Request* (Mar. 25, 2013)¹¹ (responses to public records requests sent to roughly 250 local law enforcement agencies show that “few agencies consistently obtain warrants” for CSLI). The volume of warrantless requests for CSLI and the ubiquity of cell phones make the question presented one of compelling national importance.

Judge Kozinski has summarized the situation well. In an opinion written six years ago, he began by noting that this Court’s decision in *United States v. Knotts*, 460 U.S. 276, 283–84 (1983), expressly left open the question whether “‘twenty-four hour surveillance of any citizen of this country’ by means of ‘dragnet-type law enforcement practices’ violates the Fourth Amendment’s guarantee of personal privacy.” *United States v. Pineda-Moreno*, 617 F.3d

¹¹ <https://www.aclu.org/cases/cell-phone-location-tracking-public-records-request>.

1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing *en banc*). He then cogently observed, “[w]hen requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that ‘such dragnet-type law enforcement practices’ are already in use.” *Id.* What was true six years ago is even more true today. This Court’s intervention is needed now to ensure that the Fourth Amendment does not become a dead letter as police accelerate their warrantless access to rich troves of sensitive personal location data.

II. FEDERAL COURTS OF APPEALS AND STATE HIGH COURTS ARE DIVIDED.

The Sixth Circuit’s decision in this case widens the conflict over whether, or in what circumstances, sensitive cell phone location data held in trust by a service provider is protected by a warrant requirement.

A. The Circuits Are Split Over Whether the Third-Party Doctrine Eliminates People’s Reasonable Expectation of Privacy in Their Historical CSLI.

The Sixth Circuit joins the Fourth, Fifth, and Eleventh Circuits in holding that there is no reasonable expectation of privacy in historical cell site location information under the Fourth Amendment, and therefore that no warrant is required. In the first of these decisions, *In re Application of the U.S. for Historical Cell Site Data*,

724 F.3d 600 (5th Cir. 2013), a magistrate judge rejected a government application for an order pursuant to the Stored Communications Act, 18 U.S.C. § 2703(d), seeking historical CSLI, holding that a warrant is required under the Fourth Amendment. On appeal, a divided panel of the Fifth Circuit held that any expectation of privacy in CSLI is vitiated by the cell service provider's creation and possession of the records. 724 F.3d at 613. The court rejected the argument that cell phone users retain an expectation of privacy in the data because they do not voluntarily convey their location information to the service provider. *Id.* at 613–14; *see also United States v. Guerrero*, 768 F.3d 351, 358–59 (5th Cir. 2014) (applying *In re Application* in the context of a suppression motion). The Fourth and Eleventh Circuits have subsequently agreed with this position. *Graham*, 824 F.3d at 424–25; *Davis*, 785 F.3d at 511–13.

The Third Circuit takes the contrary position. *See Fifth Circuit CSLI Opinion*, 724 F.3d at 616 (Dennis, J., dissenting) (recognizing split between Third and Fifth Circuits). In a decision issued more than a year before this Court's opinion in *Jones*, the Third Circuit held that magistrate judges have discretion to require a warrant for historical CSLI if they determine that the location information sought will implicate the suspect's Fourth Amendment privacy rights by showing, for example, when a person is inside a constitutionally protected space. *Third Circuit CSLI Opinion*, 620 F.3d at 319. In reaching that conclusion, the court rejected the argument that a cell phone user's expectation of privacy is eliminated by the service provider's ability to access that 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.”

Id. at 317–18 (last alteration in original). Therefore, the court held, the third-party doctrine does not apply to historical CSLI records. *Id.*

This split in the circuits is accentuated by the growing number of states that require a warrant for historical CSLI by statute or pursuant to judicial opinion. *See Zanders v. State*, No. 15A01–1509–CR–1519, __ N.E.3d __, 2016 WL 4140998 (Ind. Ct. App. Aug. 4, 2016); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); Colo. Rev. Stat. § 16-3-303.5(2); Me. Rev. Stat. tit. 16, § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); Utah Code Ann. § 77-23c-102(1)(a); N.H. Rev. Stat. Ann. § 644-A:2; 2016 Vt. Laws No. 169 (S. 155) (to be codified at Vt. Stat. Ann. tit. 13, § 8102(b)). Additional states require a warrant for real-time cell phone location data. *See, e.g., Tracey v.*

State, 152 So. 3d 504 (Fla. 2014); *State v. Earls*, 70 A.3d 630 (N.J. 2013); 725 Ill. Comp. Stat. 168/10; Ind. Code 35-33-5-12; Md. Code Ann. Crim. Proc. § 1-203.1(b); Va. Code Ann. § 19.2-70.3(C). Requiring a warrant for CSLI would harmonize the protections available to people throughout the United States.

B. The Circuits Are Split Over Whether There is a Reasonable Expectation of Privacy in Longer-Term Location Information Collected by Electronic Means.

In *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945, the D.C. Circuit held that using a GPS device to surreptitiously track a car over the course of 28 days violates reasonable expectations of privacy and is therefore a Fourth Amendment search. *Id.* at 563. The court explained that “[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation.” *Id.* at 562. Therefore, people have a reasonable expectation of privacy in the intimate and private information revealed by “prolonged GPS monitoring.” *Id.* at 563.

Although this Court affirmed on other grounds, relying on a trespass-based rationale, the D.C. Circuit’s approach under the *Katz* reasonable-expectation-of-privacy test remains controlling law in

that circuit.¹² And that holding does not depend on the nature of the tracking technology at issue: prolonged electronic surveillance of the location of a person’s cell phone is at least as invasive as prolonged electronic surveillance of the location of her car. *See Jones*, 132 S. Ct. at 963 (Alito, J., concurring in the judgment) (explaining that law enforcement access to cell phone location information is “[p]erhaps most significant” of the “many new devices that permit the monitoring of a person’s movements.”).

The Sixth Circuit rejected this reasoning when it held that the information contained in CSLI records is categorically unprotected by the Fourth Amendment, regardless of what it reveals and over what period of time. Pet. App. 13a–14a. In doing so, the court of appeals widened the circuit split over whether people have a reasonable expectation of privacy in their longer-term location information—a split that existed prior to *Jones* and continues today. *Compare Maynard*, 615 F.3d at 563 (prolonged electronic location tracking is a search under the Fourth Amendment), *with Pineda-Moreno*, 591 F.3d at 1216–1217 (prolonged electronic location tracking is not a search under the Fourth Amendment), *United States v. Garcia*, 474 F.3d 994, 996–99 (7th Cir. 2007) (same), and *United States v. Marquez*, 605 F.3d 604, 609 (8th Cir. 2010) (“A person traveling via automobile on public streets has no reasonable

¹² *See* Will Baude, *Further Thoughts on the Precedential Status of Decisions Affirmed on Alternate Grounds*, The Volokh Conspiracy (Dec. 3, 2013, 7:27 PM), <http://volokh.com/2013/12/03/thoughts-precedential-status-decisions-affirmed-alternate-grounds/>.

expectation of privacy in his movements from one locale to another.”).

III. THE SIXTH CIRCUIT ERRED IN HOLDING THAT THE CONDUCT HERE WAS NOT A SEARCH.

A. The Sixth Circuit Erred in Holding That There Is No Reasonable Expectation of Privacy in Historical CSLI.

The Sixth Circuit majority held that the mere fact that the government obtained the CSLI records from Petitioner’s service provider, rather than from Petitioner himself, dooms his Fourth Amendment claim in light of *United States v. Miller* and *Smith v. Maryland*. Neither *Miller* nor *Smith* compels that conclusion and this Court should reject that understanding of its prior precedent. The mere fact that another person or entity has access to or control over private records does not in itself—and without regard to any other circumstance—destroy an otherwise reasonable expectation of privacy. Though third-party access to records may be one factor weighing on the *Katz* reasonable-expectation-of-privacy analysis, the third-party doctrine elucidated in *Miller* and *Smith* is not and never has been an on-off switch. See *Florida v. Jardines*, 133 S. Ct. 1409, 1418–19 (2013) (Kagan, J., concurring) (expectation of privacy in odors detectable by a police dog that emanate from a home); *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (information about location and movement in public, even though exposed to public view); *Kyllo*, 533 U.S. 27 (thermal signatures emanating from a home); *Ferguson v. City*

of *Charleston*, 532 U.S. 67, 78 (2001) (“The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.”); *Bond v. United States*, 529 U.S. 334, 336 (2000) (bag exposed to the public on luggage rack of bus); *Minnesota v. Olson*, 495 U.S. 91, 98–99 (1990) (“an overnight guest has a legitimate expectation of privacy in his host’s home” even though his possessions may be disturbed by “his host and those his host allows inside”); *United States v. Jacobsen*, 466 U.S. 109, 115 (1984) (reasonable expectation of privacy in letters and sealed packages entrusted to private freight carrier); *Katz v. United States*, 389 U.S. 347 (1967) (reasonable expectation of privacy in contents of phone call even though call is conducted over private companies’ networks); *Stoner v. California*, 376 U.S. 483, 487–90 (1964) (implicit consent to janitorial personnel to enter motel room does not amount to consent for police to search room); *Chapman v. United States*, 365 U.S. 610, 616–17 (1961) (search of a house invaded tenant’s Fourth Amendment rights even though landlord had authority to enter house for some purposes).

The Sixth Circuit erred in treating the fact of third party access to the records as dispositive. Pet. App. 14a. This Court should make clear that the reasonable-expectation-of-privacy test relies on a totality-of-the-circumstances analysis. Avoiding mechanical applications of holdings from the analog age is of paramount importance when dealing with highly sensitive and voluminous digitized records. See *Riley*, 134 S. Ct. at 2489. It is virtually impossible to participate fully in modern life without

leaving a trail of digital breadcrumbs that create a pervasive record of the most sensitive aspects of our lives. Ensuring that technological advances do not “erode the privacy guaranteed by the Fourth Amendment,” *Kyllo*, 533 U.S. at 34, requires nuanced applications of analog-age precedents.

This is not to say that proper resolution of this case requires wholesale rejection of *Smith* and *Miller*’s holdings. Even on the plain terms of those decisions, Petitioner retains a reasonable expectation of privacy in his CSLI.

To assess an individual’s expectation of privacy in records held by a third party this Court has looked to, among other factors, whether the records were “voluntarily conveyed” to that entity, *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 744, and what privacy interest a person has in the information the records reveal, *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 741–42. Unlike the dialed phone numbers and limited bank records at issue in *Smith* and *Miller*, “[a] cell phone customer has not ‘voluntarily’ shared his location information with a cellular provider in any meaningful way.” *Third Circuit CSLI Opinion*, 620 F.3d at 317. Location information is not entered by the user into the phone, nor otherwise affirmatively transmitted to the service provider. This is doubly true when a person receives a call, thereby taking *no* action that would knowingly or voluntarily reveal location. *Id.* at 317–18. It is also particularly clearly the case when that person’s cell phone is roaming on another carrier’s network, as was Carpenter’s here, because “[t]ypically, a cell phone user does not know when her phone is roaming onto another provider’s

network, much less the name of the other provider on whose network her phone is roaming.” *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1028–29 (N.D. Cal. 2015), *appeal dismissed*, No. 15-16760 (9th Cir. Feb. 5, 2016). “As a result, cell phone users, unlike a bank depositor or telephone dialer, will often not know the identity of the third party to which they are supposedly conveying information.” *Id.* at 1029.

Moreover, the documentation of a person’s movements, locations, and activities over the course of time contained in CSLI records is exceedingly sensitive and private in ways that were not at issue in *Smith* or *Miller*. This is so for at least two reasons. First, because people carry their phones with them virtually everywhere they go, including inside their homes and other constitutionally protected spaces, cell phone location records can reveal information about presence, location, and activity in those spaces. *See United States v. Davis*, 754 F.3d 1205, 1215–16 (11th Cir. 2014) (Sentelle, J.), *rev’d en banc*, 785 F.3d 498 (11th Cir. 2015). In *United States v. Karo*, 468 U.S. 705 (1984), this Court held that location tracking implicates Fourth Amendment privacy interests when 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 714–16. Such location tracking “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; *see also Kyllo*, 533 U.S. at 36 (use of thermal imaging device to learn information about interior of home constitutes a search).

Second, CSLI reveals a great sum of sensitive and private information about a person’s movements and activities in public and private spaces that, at least over the longer term, violates expectations of privacy. In *Jones*, although the majority opinion relied on a trespass-based rationale to determine that a search had taken place, 132 S. Ct. at 949, it specified that “[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* [reasonable-expectation-of-privacy] analysis.” *Id.* at 953. Five Justices conducted a *Katz* analysis, and concluded that at least longer-term location tracking violates reasonable expectations of privacy. *Id.* at 960, 964 (Alito, J., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring).

This conclusion did not depend on the particular type of tracking technology at issue in *Jones*. As Justice Sotomayor explained, electronic location tracking implicates the Fourth Amendment because it “generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.” *Id.* at 955. This Court subsequently amplified that point when it explained that cell phone location data raises particularly acute privacy concerns because it “can reconstruct someone’s specific movements down to

the minute, not only around town but also within a particular building.” *Riley*, 134 S. Ct. at 2490 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

The records obtained by the government in this case implicate both the expectation of privacy in private spaces and the expectation of privacy in longer-term location information. They allow the government to know or infer when a person slept at home and when he didn’t. *Davis*, 785 F.3d at 540–41 (Martin, J., dissenting). They show a person’s movements around town, nearly down to the minute.¹³ *Id.* They even allow the government to learn who a person associated with and when. *See, e.g.*, Pet. App. 81a–82a (concluding that co-defendants were at the same location based on their CSLI records); Trial Tr. 107, Dec. 16, 2013, ECF No. 333 (same).

It is not surprising, therefore, that polling data shows that more than 80 percent of people consider

¹³ Even knowing only 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. *See, e.g.*, Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Syss. Design & Implementation 20 (2011), https://www.usenix.org/legacy/events/nsdi11/tech/full_papers/Thiagarajan.pdf?CFID=230550685&CFTOKEN=76524860 (describing one algorithm for accurate trajectory interpolation using cell site information). Law enforcement routinely uses cell site data for this purpose; in this case, the government presented testimony explaining that cell site data points revealed Carpenter’s trajectories placing him at the businesses in question at the relevant times. *See* Trial Tr. 55, 57, 62, Dec. 13, 2013, ECF No. 332.

“[d]etails of [their] physical location over time” to be “sensitive”—evincing greater concern over this information than over the contents of their text messages, a list of websites they have visited, or their relationship history.¹⁴ 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*, 152 So. 3d at 522 (internal quotation marks omitted).

B. The Sixth Circuit Erred In Deferring to Congress’s 30-Year-Old Legislative Scheme.

In concluding that the Fourth Amendment does not protect people’s cell site location records from warrantless search, the Sixth Circuit majority explained that “Congress has specifically legislated on the question before us today, and in doing so has struck the balance reflected in the Stored Communications Act.” Pet. App. 15a. Thus, “society itself—in the form of its elected representatives in Congress—has already struck a balance that it thinks reasonable.” *Id.* at 16a. Therefore, the majority wrote, “[t]here is considerable irony in [a] request” to “declare that balance unconstitutional.” *Id.* at 15a.

¹⁴ Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 32, 34 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerception_sofPrivacy_111214.pdf.

The supposed balance to which the majority refers is decades old, and is a relic of legislation passed before the proliferation of cell phones and the availability of large volumes of increasingly precise cell site location information. When Congress passed the Stored Communications Act in 1986,¹⁵ there were a mere 1,000 cell sites in the United States¹⁶ (compared to more than 300,000 today)¹⁷ and less than one half of one percent of Americans had a cell phone.¹⁸ Congress gave no indication that it even considered the existence of historical CSLI, not to mention the possibility that law enforcement might want to access it. When Congress amended the Stored Communications Act in 1994,¹⁹ cellular networks were still fragmented and rudimentary, with less than 18,000 cell sites across the country.²⁰ Congress simply did not contemplate the contemporary ubiquity of cell phones and the volume

¹⁵ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848.

¹⁶ Andrea Meyer, *30th Anniversary of the First Commercial Cell Phone Call*, Verizon (Oct. 11, 2013), <https://www.verizonwireless.com/news/article/2013/10/30th-anniversary-cell-phone.html> and https://www.slideshare.net/slideshow/embed_code/27105077?rel=0

¹⁷ CTIA – The Wireless Association, *Annual Wireless Industry Survey*.

¹⁸ Meyer, *30th Anniversary of the First Commercial Cell Phone Call*.

¹⁹ Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 207, 108 Stat. 4279 (1994).

²⁰ *Background on CTIA's Wireless Industry Survey 2*, CTIA-The Wireless Association (2014), http://www.ctia.org/docs/default-source/Facts-Stats/ctia_survey_ye_2013_graphics-final.pdf.

and precision of CSLI when crafting the SCA. Courts should not give undue weight to this outdated legislative scheme in evaluating people’s reasonable expectation of privacy under the Fourth Amendment.

Moreover, in concluding that acquisition of historical CSLI is a Fourth Amendment search, a court need not hold the Stored Communications Act unconstitutional. The SCA contains a mechanism for law enforcement to obtain a warrant for CSLI. *See* 18 U.S.C. § 2703(c)(1)(A). “Section 2703(c) may be fairly construed to provide for ‘warrant procedures’ to be followed when the government seeks customer records that may be protected under the Fourth Amendment, including historical cell site location information.” *Fifth Circuit CSLI Opinion*, 724 F.3d at 617 (Dennis, J., dissenting). The determination that “one proposed interpretation or use of the SCA as applied did not comply with the Fourth Amendment’s requirement for a warrant based on probable cause” is firmly within the purview of the judiciary. Pet. App. 32a (Stranch, J., concurring). Indeed, “[t]he question before [the court] is one that courts routinely answer: did the search at issue require a warrant?” *Id.* at 31a–32a. This Court should provide a “simple” answer—“get a warrant.” *Riley*, 134 S. Ct. at 2495.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully Submitted,

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Steven R. Shapiro
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street,
Suite 1400
Detroit, MI 48226

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES
UNION FUND OF
MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Dated: September 26, 2016