

No. _____

IN THE

Supreme Court of the United States

◆◆◆

QUARTAVIOUS DAVIS,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

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

PETITION FOR A WRIT OF CERTIORARI

Steven R. Shapiro
Nathan Freed Wessler
Jameel Jaffer
Ben Wizner
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004

Nancy Abudu
ACLU FOUNDATION OF
FLORIDA, INC.
4500 Biscayne Boulevard,
Suite 340
Miami, FL 33137

Benjamin James Stevenson
ACLU FOUNDATION OF
FLORIDA, INC.
P.O. Box 12723
Pensacola, FL 32591-2723

David Oscar Markus
Counsel of Record
MARKUS/MOSS PLLC
40 N.W. 3rd Street,
Penthouse One
Miami, FL 33128
(305) 379-6667
dmarkus@markuslaw.com

Jacqueline E. Shapiro
40 N.W. 3rd Street,
Penthouse One
Miami, FL 33128

Attorneys for Petitioner

QUESTIONS PRESENTED

In this case, as in thousands of cases each year, the government sought and obtained the 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 67 days of Petitioner’s cell phone location records, including more than 11,000 separate location data points. Reversing a unanimous panel opinion, a majority of the *en banc* Eleventh Circuit held that there is no reasonable expectation of privacy in these location records and, even if there were such an expectation, a warrantless search would be reasonable nonetheless.

The Questions Presented are:

- 1) 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 67 days is permitted by the Fourth Amendment.
- 2) Whether the good-faith exception to the exclusionary rule applies where the search was based on a court order sought by a prosecutor rather than a warrant sought by police, particularly when the

governing statute provided the prosecutor with the option to pursue a warrant but the prosecutor ignored it.

TABLE OF CONTENTS

QUESTIONS PRESENTED	i
TABLE OF AUTHORITIES	vi
OPINIONS BELOW	1
JURISDICTION	1
RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS.....	1
STATEMENT OF THE CASE.....	4
REASONS FOR GRANTING THE WRIT	14
I. THE QUESTION PRESENTED IS ONE OF NATIONAL IMPORTANCE, OVER WHICH COURTS ARE DIVIDED.....	14
A. The Question Presented Is One Of National Importance.....	14
B. Federal Courts of Appeals and State High Courts Are Divided Over Several Issues.....	22
1. State and federal courts in Florida are split over the existence of a reasonable expectation of privacy in CSLI	22
2. The circuits are split over whether the third-party doctrine eliminates people's reasonable expectation of privacy in their historical CSLI	24
3. The circuits are split over whether there is a reasonable expectation of privacy in longer-term location	

information collected by electronic means	26
4. The circuits are split over whether the warrant requirement applies when there is a reasonable expectation of privacy in CSLI or other electronically collected location information	28
II. THE EN BANC ELEVENTH CIRCUIT ERRED IN HOLDING THAT THE CONDUCT HERE WAS NOT A SEARCH	29
A. The Eleventh Circuit Erred in Holding That There Is No Reasonable Expectation of Privacy in Historical CSLI.....	29
B. The Eleventh Circuit Erred in Holding That Even if There Is a Reasonable Expectation of Privacy in Historical CSLI, Warrantless Search is Nonetheless Reasonable.....	34
III. THE ELEVENTH CIRCUIT ERRED BY APPLYING THE GOOD-FAITH EXCEPTION TO THE EXCLUSIONARY RULE.....	36
CONCLUSION	39
APPENDIX.....	1a
Opinion, United States Court of Appeals for the Eleventh Circuit (<i>En Banc</i>) (May 5, 2015)	1a
Opinion, United States Court of Appeals for the Eleventh Circuit (June 11, 2014)	102a

Order Denying Motion to Suppress, United States District Court for the Southern District of Florida, (January 31, 2012)	137a
Order Denying Renewed Motion to Suppress, United States District Court for the Southern District of Florida (February 7, 2012)	140a
Government's Application for Stored Cell Site Information (February 2011).....	143a
Order Granting Government's Application for Stored Cell Site Information, United States District Court for the Southern District of Florida (February 2, 2011).....	151a
Excerpt of Petitioner's Historical Cell Site Location Information Records Obtained by the Government (Government Trial Exhibit 35)	154a

TABLE OF AUTHORITIES

CASES

<i>Arizona v. Gant,</i> 556 U.S. 332 (2009)	35
<i>Bond v. United States,</i> 529 U.S. 334 (2000)	30
<i>Chapman v. United States,</i> 365 U.S. 610 (1961)	30
<i>City of Indianapolis v. Edmond,</i> 531 U.S. 32 (2000)	35
<i>City of Los Angeles v. Patel,</i> 135 S. Ct. 2443 (2015)	35
<i>Commonwealth v. Augustine,</i> 4 N.E.3d 846 (Mass. 2014)	23, 28
<i>Davis v. United States,</i> 131 S. Ct. 2419 (2011)	36, 39
<i>Ferguson v. City of Charleston,</i> 532 U.S. 67 (2001)	29
<i>Florida v. Jardines,</i> 133 S. Ct. 1409 (2013)	29
<i>Illinois v. Krull,</i> 480 U.S. 340 (1987)	38
<i>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</i> , 620 F.3d 304 (3d Cir. 2010).....	21, 25, 31
<i>In re Application of the U.S. for Historical Cell Site Data</i> , 724 F.3d 600 (5th Cir. 2013)	21, 24, 34

<i>In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information,</i> 736 F. Supp. 2d 578 (E.D.N.Y. 2010).....	38
<i>In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,</i> 534 F. Supp. 2d 585 (W.D. Pa. 2008).....	38
<i>In re Application of U.S. for Historical Cell Site Data,</i> 747 F. Supp. 2d 827 (S.D. Tex. 2010)	38
<i>Katz v. United States,</i> 389 U.S. 347 (1967)	30, 32, 33
<i>Kyllo v. United States,</i> 533 U.S. 27 (2001)	15, 29, 31, 32
<i>Minnesota v. Olson,</i> 495 U.S. 91 (1990)	30
<i>New York v. Belton,</i> 453 U.S. 454 (1981)	22
<i>People v. Weaver,</i> 909 N.E.2d 1195 (N.Y. 2009)	28
<i>Riley v. California,</i> 134 S. Ct. 2473 (2014)	<i>passim</i>
<i>Samson v. California,</i> 547 U.S. 843 (2006)	35
<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, 28
<i>Stoner v. California,</i> 376 U.S. 483 (1964)	30

<i>Tracey v. State</i> , 152 So. 3d 504 (Fla. 2014).....	22, 23, 28, 34
<i>United States v. Chadwick</i> , 433 U.S. 1 (1977)	36
<i>United States v. Garcia</i> , 474 F.3d 994 (7th Cir. 2007)	28
<i>United States v. Guerrero</i> , 768 F.3d 351 (5th Cir. 2014)	24
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984)	30
<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)	32
<i>United States v. Knotts</i> , 460 U.S. 276 (1983)	18
<i>United States v. Leon</i> , 468 U.S. 897 (1984)	36, 37
<i>United States v. Marquez</i> , 605 F.3d 604 (8th Cir. 2010)	28
<i>United States v. Maynard</i> , 615 F.3d 544 (D.C. Cir. 2010)	26, 27, 28, 38
<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)	18, 27
<i>United States v. Skinner</i> , 690 F.3d 772 (6th Cir. 2012)	25

<i>Vernonia School Dist. 47J v. Acton,</i> 515 U.S. 646 (1995)	35
---	----

<i>Weeks v. United States,</i> 232 U.S. 383 (1914)	36
---	----

CONSTITUTION & STATUTES

U.S. Const. amend. IV	<i>passim</i>
Hobbs Act, 18 U.S.C. § 1951(a)	10
Stored Communications Act, 18 U.S.C. § 2703 et seq.....	<i>passim</i>
18 U.S.C. § 2703(c)(1)(a)	38
18 U.S.C. § 2703(c)(1)(A)	34
18 U.S.C. § 2703(c)(1)(b)	38
18 U.S.C. § 2703(d).....	<i>passim</i>
18 U.S.C. § 924(c).....	10
18 U.S.C. § 2113.....	5
2015 N.H. Laws ch. 262 (to be codified at N.H. Rev. Stat. Ann. § 644-A:2)	24
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
Utah Code Ann. § 77-23c-102(1)(a)	23
Va. Code Ann. § 19.2-70.3(C).....	24

OTHER AUTHORITIES

American Civil Liberties Union, Cell Phone Location Tracking Public Records Request (Mar. 25, 2013)	18
AT&T, <i>Transparency Report</i> (2015).....	17
Brief of <i>Amici Curiae</i> American Civil Liberties Union, et al., <i>United States v. Carpenter</i> , No. 14-1572 (6th Cir. Mar. 9, 2015), 2015 WL 11381481.....	8
CTIA – The Wireless Association, <i>Annual Wireless Industry Survey</i> (2014).....	7, 16
Daniel Solove, <i>Conceptualizing Privacy</i> , 90 Calif. L. Rev. 1087 (2002).....	21
J.A. 2668–3224, <i>United States v. Graham</i> , No. 12-4659 (4th Cir. June 24, 2013).....	17
Orin Kerr, <i>Eleventh Circuit Rules for the Feds on Cell-Site Records – But Then Overreaches</i> , Wash. Post (May 5, 2015)	28
Pew Research Ctr., <i>Public Perceptions of Privacy and Security in the Post-Snowden Era</i> (Nov. 12, 2014).....	34
Russell M. Gold, <i>Beyond the Judicial Fourth Amendment: The Prosecutor’s Role</i> , 47 U.C. Davis L. Rev. 1591 (2014).....	38
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)...	21
Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, <i>Wireless Substitution: Early Release of Estimates from the</i>	

<i>National Health Interview Survey, January–June 2014</i> (Dec. 2014)	16
T-Mobile, <i>Transparency Report for 2013 & 2014</i> (2015)	17
Verizon Wireless, <i>Law Enforcement Resource Team Guide</i> (2009)	7
Verizon, <i>Verizon’s Transparency Report for the First Half of 2015</i> (2015).....	17
Will Baude, <i>Further Thoughts on the Precedential Status of Decisions Affirmed on Alternate Grounds</i> , The Volokh Conspiracy (Dec. 3, 2013, 7:27 PM) ..	27

PETITION FOR A WRIT OF CERTIORARI

Petitioner Quartavius Davis respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Eleventh Circuit in Case No. 12-12928.

OPINIONS BELOW

The opinion of the *en banc* Eleventh Circuit (Pet. App. 1a) is reported at 785 F.3d 498. An earlier opinion of a three-judge panel of the Eleventh Circuit (Pet. App. 102a) is reported at 754 F.3d 1205. The relevant district court orders (Pet. App. 137a, 140a) were issued orally and are unpublished.

JURISDICTION

The *en banc* Eleventh Circuit issued its opinion on May 5, 2015. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment of 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 warrantless acquisition of sensitive and voluminous digital records of people’s locations and movements over time.

1. In February 2011, in the course of an investigation into seven armed robberies that occurred in the greater Miami area in 2010, an Assistant United States Attorney submitted to a magistrate judge an application for an order granting access to 67 days of Quartavius Davis’s historical cell-phone location records.¹ Pet. App. 5a–6a, 143a. The application, which was unsworn, did not seek a warrant based on probable cause, but rather an order 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 application sought to compel a number of cellular service providers to disclose records related to several suspects in the robberies, including Davis. Specifically, the application sought “stored telephone subscriber records, phone toll records, and corresponding geographic location data (cell site).” Pet. App. 6a, 143a–144a. The application recited information regarding robberies of retail businesses that occurred on August 7, August 31, September 7,

¹ Although Petitioner’s first name was spelled “Quartavious” in the case caption in the courts below, the correct spelling is “Quartavius.” See Pet. App. 2a n.1.

September 15, September 25, September 26, and October 1, 2010, in and around Miami, Florida, and asserted that the records sought were “relevant” to the investigation of those offenses.² Pet. App. 148a. Rather than restricting the request to only the days on which the robberies occurred, however, the application sought records “for the period from August 1, 2010 through October 6, 2010,” a total of 67 days. Pet. App. 149a.

The magistrate judge issued an “Order for Stored Cell Site Information” on February 2, 2011. Pet. App. 151a. The order directed MetroPCS, Davis’s cellular service provider, to produce “all telephone toll records and geographic location data (cell site)” for Davis’s phone for the period of August 1 through October 6, 2010. Pet. App. 7a–8a. MetroPCS complied, providing 183 pages of Davis’s cell phone records to the government.³ Those records show each of Davis’s incoming and outgoing calls during the 67-day period, along with the cell tower (“cell site”) and directional sector of the tower that Davis’s phone connected to at the start and end of most of the calls, which was “typically the ‘[n]earest

² Although none of the offenses under investigation were bank robberies, the application erroneously stated that the information sought was relevant to an investigation into offenses under the federal bank robbery statute, 18 U.S.C. § 2113. Pet. App. 148a–149a.

³ Sample pages from Davis’s records are included at Pet. App. 154a–158a. The full records were entered as Government Exhibit 35 at trial and were included in the parties’ joint appendix in the court of appeals.

and strongest' tower.”⁴ Pet. App. 8a, 91a (quoting Trial Tr. 221, Feb. 6, 2012, ECF No. 283).

MetroPCS also produced a list of its cell sites in Florida, providing the longitude, latitude, and physical address of each cell site, along with the directional orientation of each sector antenna. Gov’t Trial Ex. 36. By cross-referencing the information in Davis’s call detail records with MetroPCS’s cell-site list, the government could identify the area in which Davis’s phone was located and could thereby deduce Davis’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 three directional antennas that divide the cell site into three sectors, but an increasing number of towers have six sectors. Pet. App. 91a. 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.⁵ *Id.*

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,

⁴ 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.”

⁵ For example, in 2010 MetroPCS, the carrier used by Davis, operated a total of 214 cell sites comprising 714 sector antennas within Miami-Dade County. See Gov’t Trial Ex. 36.

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* (2014)⁶ (showing that the number of cell sites in the United States nearly doubled from 2003 to 2013); *id.* (wireless data usage increased by 9,228% between 2009 and 2013). This means that in urban and dense suburban areas like Miami, many sectors cover small geographic areas and therefore can provide relatively precise information about the location of a phone. Pet. App. 91a.

Although in this case MetroPCS provided only information identifying Davis's cell site and sector at the start and end of his calls, service providers increasingly retain more granular historical location data. See, e.g., Verizon Wireless, *Law Enforcement Resource Team (LERT) Guide 25* (2009)⁷ (providing sample records indicating caller's distance from cell site to within .1 of a mile). Location precision is also increasing as service providers deploy millions of "small cells," which provide service to areas as small as ten meters, and can allow callers to be located with a "high degree of precision, sometimes effectively identifying individual floors and rooms within buildings." Pet. App. 94a.

3. Davis's call detail records obtained by the government contain a wealth of location data. The records provide CSLI relating to 5,803 phone calls,

⁶ Available at <http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey>.

⁷ Available at <http://publicintelligence.net/verizon-wireless-law-enforcement-resource-team-lert-guide/>.

identifying 11,606 separate location data points (this accounts for cell site location information logged for the start and end of the calls). Pet. App. 91a. “This averages around one location data point every five and one half minutes for those sixty-seven days, assuming Mr. Davis slept eight hours a night.” *Id.* These records reveals a large volume of sensitive and private information about Davis’s locations, movements, and associations:

The amount and type of data at issue revealed so much information about Mr. Davis’s day-to-day life that most of us would consider quintessentially private. For instance, on August 13, 2010, Mr. Davis made or received 108 calls in 22 unique cell site sectors, showing his movements throughout Miami during that day. And the record reflects that many phone calls began within one cell site sector and ended in another, exposing his movements even during the course of a single phone call.

Also, by focusing on the first and last calls in a day, law enforcement could determine from the location data where Mr. Davis lived, where he slept, and whether those two locations were the same. 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.” Trial Tr. 42, Feb. 7, 2012, ECF No. 285. For example, from August 2, 2010, to August 31, 2010, Mr. Davis’s first and last call of the day were either or both placed from a single sector—purportedly his home sector. But on the night of September 2, 2010, Mr. Davis made calls at 11:41pm, 6:52am, and 10:56am—all from a location that was not his home sector. Just as Justice Sotomayor warned [in *United States v. Jones*, 132 S. Ct. 945 (2012)], Mr. Davis’s “movements [were] recorded and aggregated in a manner that enable[d] the Government to ascertain, more or less at will, . . . [his] sexual habits, and so on.” *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

Pet. App. 92a.

4. Prior to trial, Davis moved to suppress the CSLI records on the basis that their acquisition constituted a Fourth Amendment search and required a warrant. Pet. App. 8a–9a. The district court denied the motion without elaboration at the conclusion of the suppression hearing, stating that it intended to issue a written opinion on the matter at a later date. Pet. App. 138a. Davis renewed the suppression motion during trial, which the court again denied while reserving explanation until a later written opinion. Pet. App. 142a. The court never issued any written opinion explaining its denial of the motion.

At trial, the government introduced the entirety of Davis's CSLI records as evidence, Gov't Ex. 35, and relied on them to establish Davis's location on the days of the charged robberies. A detective with the Miami-Dade Police Department testified that Davis's CSLI records placed him near the sites of six of the robberies. Pet. App. 11a–12a. The detective also produced maps showing the location of Davis's phone relative to the locations of the robberies, which the government introduced into evidence. *Id.*; Gov't Ex. 37A–F. Thus, “[t]he government relied upon the information it got from MetroPCS to specifically pin Mr. Davis's location at a particular site in Miami.” Pet. App. 93a. The prosecutor asserted to the trial judge, for example, that “Mr. Davis's phone [was] literally right up against the America Gas Station immediately preceding and after [the] robbery occurred,” *id.* (quoting Trial Tr. 58, Feb. 7, 2012, ECF No. 285), and argued to the jury in closing that the records “put [Davis] literally right on top of the Advance Auto Parts one minute before that robbery took place,” Trial Tr. 13, Feb. 8, 2012, ECF No. 287.

The jury convicted Davis of two counts of conspiracy to interfere with interstate commerce by threats or violence in violation of the Hobbs Act, 18 U.S.C. § 1951(a); seven Hobbs Act robbery offenses; and seven counts of using, carrying, or possessing a firearm in each robbery in violation of 18 U.S.C. § 924(c). All but the first of the § 924(c) convictions carried mandatory consecutive minimum sentences of 25 years each. As a result, the court sentenced Davis to nearly 162 years' imprisonment (1,941

months).⁸ The court stated at sentencing that in light of Davis's young age (18 and 19 years old at the time of the offenses) and the nature of the crimes, the court believed a sentence of 40 years would have been appropriate. Sentencing Tr. 33, July 17, 2012, ECF No. 366. Because the court was afforded no discretion in sentencing, however, it sentenced Davis to 162 years in prison.

5. On appeal, a unanimous three-judge panel of the Eleventh Circuit held that the government violated Davis's Fourth Amendment rights by requesting and obtaining his historical cell site location information without a warrant. Pet. App. 102a, 118a. Writing for the panel, Judge Sentelle⁹ opined that Davis had a reasonable expectation of privacy in his CSLI because it could reveal information about his whereabouts in private spaces, thereby "convert[ing] what would otherwise be a private event into a public one." Pet. App. 119a. Judge Sentelle explained that "[t]here is a reasonable privacy interest in being near the home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute." Pet. App. 120a. The panel further held that MetroPCS's possession of Davis's CSLI did not deprive Davis of a reasonable expectation of privacy in that information because he did not voluntarily disclose his location information to the company. Pet. App. 121a–122a. The panel affirmed the district court's denial of Davis's

⁸ The court of appeals reduced the sentence for one of the counts of conviction by two years, resulting in a sentence of nearly 160 years. Pet. App. 129a–130a.

⁹ Judge Sentelle sat on the panel by designation from the D.C. Circuit.

suppression motion, however, on the grounds that the government relied in good faith on the magistrate judge’s order issued under the Stored Communications Act, and therefore the exclusionary rule did not apply. Pet. App. 122a–124a.

The government petitioned for rehearing *en banc*, and a divided Eleventh Circuit vacated the panel opinion.¹⁰ Writing for the majority, Judge Hull held that no Fourth Amendment search occurred because Davis had no reasonable expectation of privacy in cell phone location records held by his service provider. Pet. App. 30a. She further concluded that, even if a Fourth Amendment search had taken place, use of an SCA order rather than a warrant is reasonable because the privacy intrusion was minor and the government has a compelling interest in investigating crimes.¹¹ Pet. App. 40a–41a.

Five of the *en banc* court’s eleven judges expressed misgivings. Judge Jordan, joined by Judge Wilson, wrote separately to express the concern that

[a]s technology advances, location information from cellphones (and, of course, smartphones) will undoubtedly become more precise and easier to obtain, and if there is no expectation of

¹⁰ Only one member of the original panel participated in *en banc* reconsideration. Judge Sentelle was not permitted to participate because he had participated in the panel as a visitor from the D.C. Circuit. Judge Dubina has taken senior status, and opted not to participate in *en banc* reconsideration. See 11th Cir. R. 35-10.

¹¹ The court held in the alternative that the good-faith exception to the exclusionary rule applies. Pet. App. 43a n.20, 75a n.35.

privacy here, I have some concerns about the government being able to conduct 24/7 electronic tracking (live or historical) in the years to come without an appropriate judicial order.

Pet. App. 50a (internal citation omitted). Judge Jordan did not join the court's conclusion that there is no reasonable expectation of privacy in CSLI records, but concurred that a search of CSLI is reasonable if conducted with an SCA order. Pet. App. 51a.

Judge Rosenbaum also wrote separately to sound a note of caution:

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.

Pet. App. 58a.

Judge Martin, joined by Judge Jill Pryor, dissented and opined that there is a reasonable expectation of privacy in CSLI, and that law enforcement should need a warrant to access it. Pet. App. 75a–101a.

REASONS FOR GRANTING THE WRIT

I. THE QUESTION PRESENTED IS ONE OF NATIONAL IMPORTANCE, OVER WHICH COURTS ARE DIVIDED.

A. The Question Presented Is One Of National Importance.

In two of the last three 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 raises an important and pressing question left open by those decisions.

The records at issue in this case reveal extraordinarily sensitive details of a person's life, "reflect[ing] a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring). The court of appeals held that this voluminous transcript 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 this Court's third-party records decisions from the 1970s. Pet. App. 26a–30a (citing *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976)). This Court recently cautioned that "any extension of . . . reasoning [from decisions concerning analog searches] to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489. The court of

appeals did not take to heart the crucial lesson that relying blindly on “pre-digital analogue[s]” risks causing “a significant diminution of privacy.” *Id.* at 2493.

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.”).

This case raises a hotly contested question that sits at the confluence of *Jones* and *Riley*: whether the pervasive location data generated by use of a cell phone is protected from warrantless search by the Fourth Amendment. Resolution of this question is a matter of great and national importance.

1. The volume and frequency of law enforcement requests for CSLI make resolution of the question in this case of paramount importance. Cell phone use is now ubiquitous, with “[m]ore than 90% of American adults . . . own[ing] a cell phone.” *Riley*, 134 S. Ct. at 2490. As of December 2013, there were more than 335 million wireless subscriber accounts in the United States,¹² and 44 percent of U.S. households have *only* cell phones.¹³ When “nearly 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,” *Riley*, 134 S. Ct. at 2490, the privacy implications of warrantless law enforcement access to cell phone location data are difficult to overstate.

¹² CTIA – The Wireless Association, *Annual Wireless Industry Survey* (2014), available at <http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey>.

¹³ 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>.

This is not an isolated or occasional concern. Law enforcement is requesting staggering volumes of CSLI from service providers. In 2014, for example, AT&T received 64,073 requests for cell phone location information.¹⁴ Verizon received approximately 21,800 requests for cell phone location data in just the first half of 2015.¹⁵

The government often obtains large volumes of CSLI pursuant to such requests. In this case the government seized 67 days' worth of Davis's location data comprising 11,606 location data points. Pet. App. 75a. A request for two months of data is no aberration: according to T-Mobile, which now owns Davis's service provider, MetroPCS, the average law enforcement request "asks for approximately fifty-five days of records." T-Mobile, *Transparency Report for 2013 & 2014*, at 5 (2015).¹⁶ Other cases pending in the courts of appeals involve even greater quantities 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. J.A. 2668–3224, *United States v. Graham*, No. 12-4659 (4th Cir. June 24, 2013). In another case, the government obtained 127 days of CSLI containing 12,898 cell site location data

¹⁴ AT&T, *Transparency Report* 4 (2015), available at http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_January_2015.pdf.

¹⁵ Verizon, *Verizon's Transparency Report for the First Half of 2015* (2015), available at <http://transparency.verizon.com/us-report/?us-data>.

¹⁶ Available at <http://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf>.

points. Brief of *Amici Curiae* American Civil Liberties Union, et al., at 9, *United States v. Carpenter*, No. 14-1572 (6th Cir. Mar. 9, 2015), 2015 WL 1138148.

In *Jones*, Justice Alito recognized that cell phones are “[p]erhaps most significant” of the “many new devices that permit the monitoring of a person’s movements.” 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)¹⁷ (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.

Indeed, easy access to a comprehensive transcript of a person’s movements raises questions long recognized as particularly significant. “The Supreme Court in [*United States v.] Knotts*[, 460 U.S. 276, 283–84 (1983)] expressly left open 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 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing *en banc*). As Judge Kozinski has opined, “[w]hen

¹⁷ <https://www.aclu.org/cases/cell-phone-location-tracking-public-records-request>.

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.* This Court’s intervention is needed now to ensure that the Fourth Amendment does not become dead letter as police accelerate their warrantless access to rich troves of sensitive personal location data.

2. This case also squarely presents the broader question of how the protections of the Fourth Amendment apply to sensitive and private data in the hands of trusted third parties.

As Justice Sotomayor noted in *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. at 957 (Sotomayor, J., concurring). It is not necessary in this case to wholly reassess the third-party doctrine. But it is critically important to clarify the scope of analog-age precedents to digital surveillance techniques.

Lower courts are struggling with how to apply pre-digital precedents from *United States v. Miller* and *Smith v. Maryland* to newer forms of pervasive

digital data. In *Smith*, this Court held 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 739, 742. The Court relied heavily on the fact that when dialing a phone number, the caller “voluntarily convey[s] numerical information to the telephone company.” *Id.* at 744. 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). *Miller*, which involved records about a bank depositor’s transactions voluntarily conveyed to the bank, reached much the same conclusion. 425 U.S. at 440–42. 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.”

In this case, Judge Sentelle, writing for the original Eleventh Circuit panel, concluded that the third-party doctrine does not apply to CSLI because of its sensitivity and the lack of voluntary conveyance to service providers. Pet. App. 120a–122a. Judge Martin, in dissent from the *en banc* majority opinion, agreed, and expressed alarm that “the majority’s blunt application of the third-party doctrine threatens to allow the government access to a staggering amount of information that surely must be protected under the Fourth Amendment.” Pet. App. 81a. The *en banc* majority, on the other hand, concluded that this case is resolved by a straight

application of the holding of *Smith*, without regard for the significant changes in technology and expectations of privacy over the intervening 35 years. Pet. App. 26a–28a. Yet three concurring judges wrote separately to register their concerns about exempting the CSLI records at issue from Fourth Amendment protections, inviting this Court to clarify the scope of the rule announced in *Miller* and *Smith*. See Pet. App. 50a–51a (Jordan, J., concurring); *id.* at 58a–59a (Rosenbaum, J., concurring).

Other courts are similarly divided. Compare *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 612–13 (5th Cir. 2013) [“*Fifth Circuit CSLI Opinion*”] (no expectation of privacy in CSLI under *Smith*), with *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, 317 (3d Cir. 2010) [“*Third Circuit CSLI Opinion*”] (distinguishing *Smith* and holding that cell phone users may retain a reasonable expectation of privacy in CSLI).

Lower courts’ struggles to define the scope of the Fourth Amendment’s protections for newer forms of sensitive digital data are reflected in widespread 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 Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087, 1151–52 (2002). These scholars and judges have called on this Court to ensure that the Fourth

Amendment keeps pace with the rapid advance of technology.

This case presents a good vehicle for addressing application of the Fourth Amendment warrant requirement to sensitive and private records held by a third party. 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. Federal Courts of Appeals and State High Courts Are Divided Over Several Issues.

The Eleventh 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.

1. State and federal courts in Florida are split over the existence of a reasonable expectation of privacy in CSLI. In *Tracey v. State*, 152 So. 3d 504, 526 (Fla. 2014), the Supreme Court of Florida held that under the Fourth Amendment there is a reasonable expectation of privacy in real-time cell phone location data, and that accordingly a warrant is required when law enforcement seeks access to it. Although historical CSLI records were not at issue in *Tracey*, *see id.* at 516, the court concluded that the same principles that courts have held to create a reasonable

expectation of privacy in historical CSLI also require protection of real-time CSLI, *id.* at 523. Indeed, for Fourth Amendment purposes, there is little meaningful difference between historical and real-time records, as both provide information about a person’s location in private spaces and allow police to learn a large quantity of private information about a person’s activities and movements. If anything, search of historical records is more invasive because it provides law enforcement with a completely new investigative power to go backward in time and track someone’s location in the past—a veritable time machine with no analogue in the capabilities of the founding-era constabulary.

Florida law enforcement agents now must choose whether to follow the holding of *Tracey* and obtain a warrant before seizing CSLI, or to follow the Eleventh Circuit’s holding in this case and forgo the warrant requirement. And even if state and local law enforcement agencies decide that *Tracey* articulates the controlling rule, residents of Florida will remain subject to disparate Fourth Amendment protections depending on whether they are investigated by state or federal agents. The practical protections of the Fourth Amendment should not turn on which uniform the investigators are wearing.

Likewise, a number of states require a warrant for historical CSLI by statute or under their state constitution as interpreted by the state’s highest court. See *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); 2015

N.H. Laws ch. 262 (to be codified at N.H. Rev. Stat. Ann. § 644-A:2). Additional states require a warrant for real-time cell phone location data. *See, e.g., 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 in state and federal investigations in these states as well.

2. The circuits are split over whether the third-party doctrine eliminates people's reasonable expectation of privacy in their historical CSLI. The Eleventh Circuit joins the Fifth Circuit 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 *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, 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).¹⁸

The Third Circuit takes the contrary position. 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

¹⁸ The Sixth Circuit has held that the Fourth Amendment does not apply to shorter-term real-time tracking of a cell phone user's location during a single three-day multi-state trip on public highways. *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012). The court reserved decision about “situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes.” *Id.* at 780 (citing *Jones*, 132 S. Ct. at 957–64).

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.*

3. 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.¹⁹ 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 Eleventh Circuit rejected this reasoning when it opined that “reasonable expectations of privacy under the Fourth Amendment do not turn on the quantity of non-content information MetroPCS collected in its historical cell tower location records.” Pet. App. 36a. 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),

¹⁹ 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/>.

and United States v. Marquez, 605 F.3d 604, 609 (8th Cir. 2010) (“A person traveling via automobile on public streets has no reasonable expectation of privacy in his movements from one locale to another.”).

4. The circuits are split over whether the warrant requirement applies when there is a reasonable expectation of privacy in CSLI or other electronically collected location information. A majority of the *en banc* Eleventh Circuit held that, even if Petitioner had a reasonable expectation of privacy in his CSLI, the government’s warrantless seizure and search of the records was reasonable. Pet. App. 39a–43a. That alternate holding creates a split with the courts that have found there is a reasonable expectation of privacy in CSLI or other electronically collected location information, and that have required a warrant for law enforcement access to it.²⁰ See *Tracey* 152 So.3d at 526 (probable cause warrant required for tracking CSLI); *Augustine*, 4 N.E. 3d at 866 (same, under state constitution); *Earls*, 70 A.3d at 588 (same); *see also Maynard*, 615 F.3d at 566–67 (holding that warrant is required for prolonged GPS tracking of a car); *People v. Weaver*, 909 N.E.2d 1195, 1203 (N.Y. 2009) (warrant required for GPS tracking under state constitution).

²⁰ See Orin Kerr, *Eleventh Circuit Rules for the Feds on Cell-Site Records – But Then Overreaches*, Wash. Post (May 5, 2015), <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/05/eleventh-circuit-rules-for-the-feds-on-cell-site-records-but-then-overreaches/> (“[T]he en banc court’s alternative holding . . . [is] a novel development of the law that cuts against a lot of practice and precedent.”).

II. THE EN BANC ELEVENTH CIRCUIT ERRED IN HOLDING THAT THE CONDUCT HERE WAS NOT A SEARCH.

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

The Eleventh 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*. This Court should make clear that a cell service provider's ability to access customers' location data does not in itself eliminate cell phone users' reasonable expectation of privacy in that data.

The mere fact that another person or entity has access to or control over private records does not in itself 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 Eleventh Circuit erred in treating the fact of third party access to the records as dispositive. Pet. App. 26a–30a. 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.

Moreover, the transcript of a person’s movements, locations, and activities over the course of time contained in CSLI records is exceedingly sensitive and private. 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. Pet. App. 92a, 119a–120a. 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.* 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*, and Justice Alito identified the proliferation of mobile devices as “[p]erhaps most significant” of the emerging location tracking technologies. *Id.* at 963. 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 recently 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 Davis slept at home and when he didn’t. Pet. App. 92a. They show his movements around town, nearly down to the minute. *Id.* at 91a–93a. They even allow the government to learn whom he associated with and when. See Trial Tr. 13, Feb. 8, 2012, ECF No. 287.

It is not surprising, therefore, that recent polling data shows that more than 80 percent of people consider “[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. Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 32, 34 (Nov. 12, 2014).²¹ 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).²²

B. The Eleventh Circuit Erred in Holding That Even if There Is a Reasonable Expectation of Privacy in Historical CSLI, Warrantless Search is Nonetheless Reasonable.

²¹ http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

²² In concluding that acquisition of historical CSLI is a Fourth Amendment search, this 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).

In an alternate holding, the Eleventh Circuit majority concluded that even if obtaining historical CSLI is a Fourth Amendment search, warrantless seizure and search of the records is reasonable without a warrant. Pet. App. 39a–43a. That conclusion conflicts with this Court’s longstanding admonition that warrantless searches are “*per se* unreasonable . . . subject only to a few specifically established and well-delineated exceptions.” *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2452 (2015) (quoting *Arizona v. Gant*, 556 U.S. 332, 338 (2009)) (alteration in original).

This Court has recognized that certain searches outside the scope of traditional law enforcement, or aimed at categories of people under circumstances where they enjoy reduced expectations of privacy, may not require probable cause warrants. *See City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000). Here, however, no “special need” beyond normal law enforcement was served by the request for Petitioner’s CSLI. Instead, even the *en banc* Eleventh Circuit acknowledged that the government’s search of Petitioner’s CSLI served “[t]he societal interest in promptly apprehending criminals and preventing them from committing future offenses.” Pet. App. 42a. Nor did Petitioner have a reduced expectation of privacy justifying rejection of the warrant requirement. Compare *Samson v. California*, 547 U.S. 843, 850 (2006) (parolees); *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646 (1995) (student athletes). The Eleventh Circuit’s alternate holding thus conflicts with longstanding precedent of this Court.

III. THE ELEVENTH CIRCUIT ERRED BY APPLYING THE GOOD-FAITH EXCEPTION TO THE EXCLUSIONARY RULE.

The Eleventh Circuit held that, even if warrantless acquisition of Petitioner's historical cell phone location records violated the Fourth Amendment, denial of the suppression motion would have been proper because the government relied in good faith on the magistrate judge's issuance of an order under the Stored Communications Act. Pet. App. 43a n.20, 75a n.35, 122a–124a. In doing so, the court cited *United States v. Leon*, 468 U.S. 897 (1984), which held that evidence will not be suppressed if obtained by police in reliance on a facially valid warrant that later was invalidated. Here, however, the government did not seek or rely on a warrant; it relied on a court order obtained without reference to probable cause. Further, it was a prosecutor charged with knowing and upholding the Constitution, rather than a police officer “engaged in the often competitive enterprise of ferreting out crime,” *United States v. Chadwick*, 433 U.S. 1, 9 (1977), who sought and obtained the order. Therefore, the good-faith exception to the exclusionary rule does not apply.

Without the exclusionary rule, the Fourth Amendment would be “of no value” and “might as well be stricken from the Constitution.” *Weeks v. United States*, 232 U.S. 383, 393 (1914). Nonetheless, the exclusionary rule does not apply automatically. The purpose of the rule “is to deter future Fourth Amendment violations.” *Davis v. United States*, 131 S. Ct. 2419, 2426 (2011). That purpose would be

served by suppressing the unconstitutionally obtained evidence here.

The reasoning of *Leon* does not extend to the circumstances of this case for two reasons. First, the role of the judge is different. In *Leon*, the judge's role in considering a probable cause affidavit and issuing a warrant was to assess the adequacy of the factual probable cause recitation in the officer's sworn declaration and to determine whether the warrant was sufficiently particularized. Those are decisions well within the competence and experience of a judge when acting ex parte.

When considering an application for a 2703(d) order, however, an additional question arises, one ill-suited to an ex parte proceeding. The judge must decide whether the records requested are properly obtainable with such an order, or whether a warrant is required by the Fourth Amendment instead. But considering legal arguments of that nature in an ex parte proceeding, with only the government in attendance, places the court at the government's mercy. When a prosecutor makes the choice to submit an application under 18 U.S.C. § 2703(d) seeking CSLI, without alerting the court to the possible constitutional deficiency of such application, she should bear the risk of the court being ignorant of arguments on the other side, and of the order being subsequently ruled unconstitutional.

Second, suppression will provide deterrence because, unlike in *Leon* where the *police* relied on the warrant, here a *prosecutor* was the relevant actor. Unlike police, a prosecutor, as an attorney and officer of the court, “may properly be charged with knowledge[] that the search was unconstitutional

under the Fourth Amendment.” *Illinois v. Krull*, 480 U.S. 340, 348–49 (1987) (citation omitted). Prosecutors are bound “to interpret the Constitution” and to “enforce the law within constitutional boundaries.” Russell M. Gold, *Beyond the Judicial Fourth Amendment: The Prosecutor’s Role*, 47 U.C. Davis L. Rev. 1591, 1623 (2014).

The Stored Communications Act makes available to the government two relevant types of legal process: a court order based on “reasonable grounds” that the records sought are “relevant and material” to an investigation, 18 U.S.C. § 2703(c)(1)(b), (d); and a probable cause warrant, *id.* § 2703(c)(1)(a). By the time the prosecutor applied for the SCA order in this case in February 2011, a number of magistrate judges had held that the Fourth Amendment compels the government to use the warrant mechanism under the SCA rather than an order under § 2703(d), casting the constitutionality of the latter procedure in significant doubt. *See, e.g., In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010); *In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, 736 F. Supp. 2d 578 (E.D.N.Y. 2010), *rev’d without explanation*, Nov. 29, 2010; *In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t*, 534 F. Supp. 2d 585 (W.D. Pa. 2008) (opinion joined by all magistrate judges in the district), *vacated and remanded for further factfinding and analysis*, 620 F.3d 304 (3d Cir. 2010). The D.C. Circuit had also decided *Maynard*, holding that longer-term electronic location tracking is a Fourth Amendment search. 615 F.3d 544.

In light of these authorities, a cautious and responsible prosecutor should have known that seeking historical CSLI using a § 2703(d) order seriously risked violating the Constitution. The prudent course would have been to seek a warrant instead. Suppressing the evidence in this case would deter future violations by incentivizing prosecutors to choose the more constitutionally valid course when faced with a decision of what legal process to use.²³

CONCLUSION

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

Respectfully Submitted,

David Oscar Markus
Counsel of Record
MARKUS/MOSS PLLC
40 N.W. 3rd Street,
Penthouse One
Miami, FL 33128
(305) 379-6667
dmarkus@markuslaw.com

²³ Even if the Court determines that the good-faith exception applies, it should still grant certiorari to decide the underlying Fourth Amendment question. As this Court has explained, “applying the good-faith exception in this context will not prevent judicial reconsideration of prior Fourth Amendment precedents.” *Davis*, 131 S. Ct. at 2433. Unless the Court opines on what the Fourth Amendment means and requires in the context of searches based on new and evolving technologies, the law will stagnate and law enforcement and the public will be left without the guidance they so acutely require.

Jacqueline E. Shapiro
40 N.W. 3rd Street,
Penthouse One
Miami, FL 33128

Steven R. Shapiro
Nathan Freed Wessler
Jameel Jaffer
Ben Wizner
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004

Nancy Abudu
ACLU FOUNDATION OF
FLORIDA, INC.
4500 Biscayne Blvd.,
Ste. 340
Miami, FL 33137

Benjamin James Stevenson
ACLU FOUNDATION OF
FLORIDA, INC.
P.O. Box 12723
Pensacola, FL 32591-2723

Dated: July 30, 2015