No. 16-6308

IN THE

Supreme Court of the United States

AARON GRAHAM,

Petitioner,

v.

UNITED STATES,

Respondent.

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

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, BRENNAN CENTER FOR JUSTICE, CENTER FOR DEMOCRACY & TECHNOLOGY, THE CONSTITUTION PROJECT, AND NATIONAL COALITION TO PROTECT CIVIL FREEDOMS IN SUPPORT OF PETITIONER

RACHEL LEVINSON-WALDMAN
MICHAEL W. PRICE
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Avenue of the Americas,
12th Floor
New York, New York 10013
(646) 292-8335

JENNIFER LYNCH
Counsel of Record
ANDREW CROCKER
JAMIE WILLIAMS
STEPHANIE LACAMBRA
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
jlynch@eff.org

Attorneys for Amici Curiae

268807

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

CASES

Cited Authorities

Page

Cited Authorities

Page

Page

STATUTES

OTHER AUTHORITIES

Page

Page

CONSTITUTIONAL PROVISIONS

Page

LEGISLATIVE AUTHORITIES

STATEMENT OF INTEREST[1]

Amici are organizations committed to ensuring constitutional rights continue to be protected as technology advances and include the Electronic Frontier Foundation, the Brennan Center for Justice at NYU School of Law, the Center for Democracy & Technology, the Constitution Project, and the National Coalition to Protect Civil Freedoms. Many of these organizations have appeared previously as *amicus curiae* before this Court. Their individual organizational statements are contained in the Appendix following this brief.

INTRODUCTION

Cell phones have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S.Ct. 2473, 2484 (2014). In *Riley*, this Court recognized that the ubiquity of cell phones, combined with their capacity to hold vast quantities of detailed personal information—potentially the "sum of an individual's private life"—makes cell phones so qualitatively and quantitatively different from their analog counterparts as to require a warrant prior to search. *Id.* at 2489.

---

1. Pursuant to Supreme Court Rule 37.2(a), *amici* have provided timely notice to all counsel, and all parties consent to the filing of this brief. Pursuant to Supreme Court Rule 37.6, *amici* state this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than *amici* or their counsel made a monetary contribution to fund the preparation or filing of this brief.

However, the private information available from cell phones is not limited to the data stored on the phone itself. For a phone to receive and share much of that data—in other words, to be usable—it must connect with a cell tower. Every time it does, it generates information, stored by the phone company, about which tower the phone connected to—essentially where the phone was—on a given date and time. These small bits of data—called cell site location information (CSLI)—are aggregated by providers and, like GPS data that may be stored on the phone itself, "generate[] 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." *United States v. Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring).

CSLI is proving increasingly useful to law enforcement. As cell phone use has increased, so too has the number of cell towers or cell "sites," leading to increasingly precise location information on individuals. Equipped with CSLI, police can now not only place suspects at specific crime scenes, but can also reconstruct almost anyone's movements for many months in the past.

The petitions for *certiorari* in *Graham v. United States*, Case No. 16-6308, and *Carpenter v. United States*, Case No. 16-402,[2] ask this Court to address whether the Fourth Amendment prohibits the warrantless seizure and search of CSLI. Both cases relied on this Court's opinion in *Smith v. Maryland*, 442 U.S. 735 (1979), to hold Americans lack a reasonable expectation of privacy in CSLI because it is a business record held by third-party

2. *Amici* believe the issues raised by both cases are substantially similar and have filed the same brief in support of both petitions for *certiorari*.

service providers. But the few days of numbers dialed in *Smith* are so qualitatively different from the months of detailed location data collected in these cases as to prove Justice Sotomayor's point that *Smith's* premise 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." *Jones*, 132 S.Ct. at 957 (Sotomayor, J. concurring).

As CSLI has become more precise and revealing, and as law enforcement increasingly relies on this data to secure criminal convictions, the time is ripe for this Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id.* The Court should grant *certiorari* to address this issue and make clear that the Fourth Amendment requires a warrant for CSLI.

ARGUMENT[3]

Americans carry their cell phones with them everywhere and, as they do, they generate increasingly granular and detailed information about where they have been and when. This data is purely a byproduct of owning and carrying an operational phone—it is created whenever the phone tries to send and receive information, generally without forethought or conscious action by the owner. And it is stored with third-party service providers who may retain it for years.

The dramatic increase in the number of cell phones and cell sites and the amount of detailed, sensitive location

3. Except where noted, all cited web sites were last visited on October 20, 2016.

data they generate, combined with the quantity and extent of law enforcement demands for this data, show that it is time for this Court to address the Fourth Amendment privacy implications of CSLI. The fact that judges within the federal and state court systems are in stark disagreement regarding whether a warrant is required to obtain this data only underscores this point.

I. The Dramatic Increase in Location Data Generated by Cell Phones, Collected by Third Parties and Available to Law Enforcement, Counsels in Favor of *Certiorari*

A. The Number of Cell Phones and Cell Sites Has Increased Significantly in the Last Thirty Years

As in *Riley*, the "element of pervasiveness that characterizes cell phones" has a crucial impact on the Fourth Amendment issues here. *Riley*, 134 S.Ct. at 2490. Today, owning a cell phone is not a luxury; more than 91% of all American adults have a cell phone, and most carry their phone with them everywhere they go.[4]

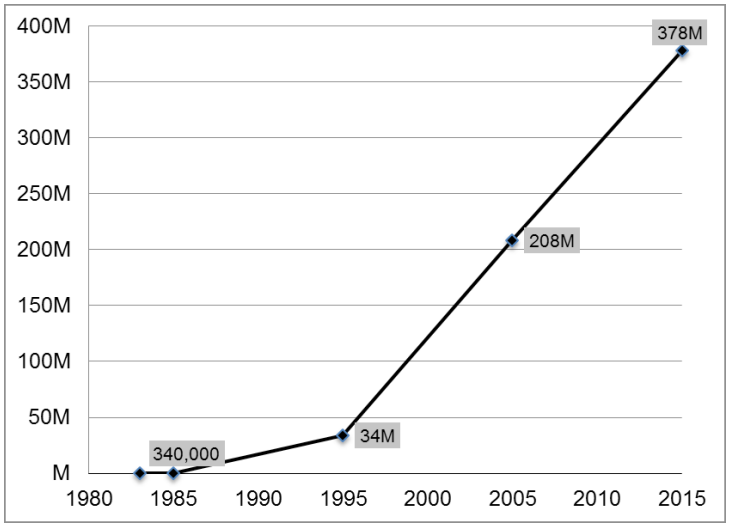
The first commercial cell phone service was offered in the United States in 1983[5]—four years after this Court's

4. *See* Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, Pew Research Center (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/; Harris Interactive, *2013 Mobile Consumer Habits Study* 2–3 (June 2013), *available at* http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf.

5. Marguerite Reardon, *Cell Phone Industry Celebrates Its 25th Birthday*, CNET (Oct. 13, 2008), https://www.cnet.com/news/cell-phone-industry-celebrates-its-25th-birthday.

seminal decision in *Smith v. Maryland* and three years before Congress enacted the Stored Communications Act ("SCA"), 18 U.S.C. §§2701–2712. Since that time, the number of mobile device accounts in the United States has grown to an estimated 378 million—53 million more accounts than people.[6]

Chart 1: Number of Mobile Device Subscriptions in United States[7]



6. CTIA—The Wireless Association, *Annual Year-End 2015 Top-Line Survey Results* 3 (May 2016) ("CTIA 2015 Survey"), *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia-survey-2015.pdf (378 million mobile device accounts); *see* U.S. Census Bureau, *U.S. and World Population Clock*, http://www.census.gov/popclock (estimated U.S. population 325 million on October 5, 2016).

7. Charts 1–3 were generated using statistics from an annual survey of wireless service providers conducted by CTIA-The Wireless Association, the leading wireless industry trade association. *See* CTIA 2015 Survey at 3.

Cell phones send and receive radio signals via base stations, known as cell towers. Towers typically have multiple cell "sites" facing in three or four different directions, each containing antennae that detect radio signals emanating from phones and that connect the phones to the cellular network.[8] Cell phones automatically try to connect to the nearest or strongest base station, and, as users move farther away from one base station and closer to another, their phones automatically transfer the connection to the new base station.

As cell phone use has increased, service providers have installed more cell sites to handle the load.[9] Estimates of the current number of cell sites in the United States range from 300,000 to 600,000.[10] These sites include an estimated 1.85 million antennae, constantly communicating with all phones in range.[11]

---

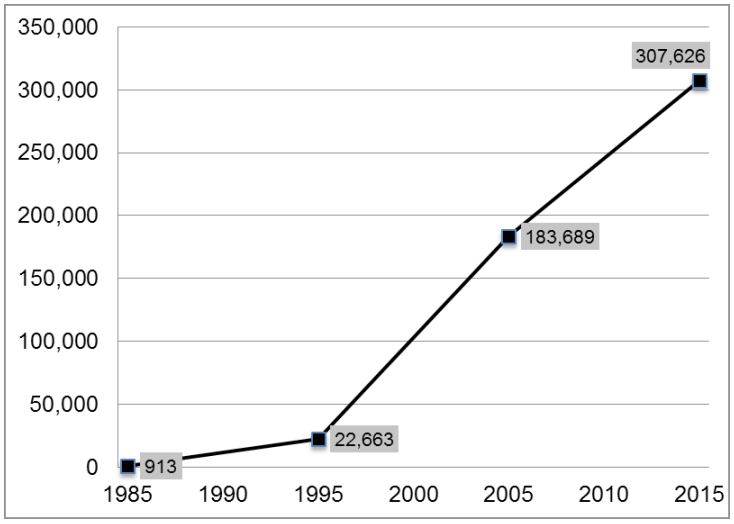
8. *See* Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary, 113th Cong. 50, at 6, 9 (2013) (written testimony of Professor Matt Blaze, University of Pennsylvania) ("Blaze Testimony"), *available at* https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf.

9. Blaze Testimony at 10 ("A sector base station can handle only a limited number of simultaneous call connections given the amount of radio spectrum 'bandwidth' allocated to the wireless carrier.").

10. CTIA 2015 Survey at 2 (307,626 cell sites in 2015); AntennaSearch.com, http://antennasearch.com (618,950 cell towers as of Oct. 2, 2016).

11. AntennaSearch.com, http://antennasearch.com (1,852,945 antennas as of Oct. 2, 2016).

Chart 2: Number of Cell Sites in United States[12]



Modern cell phones' increasing sophistication and improved capabilities have also driven the need for more cell sites. After Apple released the iPhone in 2007, "smartphones" took off. Now more than 64% of Americans own smartphones.[13] For a significant percentage of "smartphone-dependent" Americans, their phones are their only means of accessing the Internet; this is disproportionately true for young adults, people of color, and lower-income Americans.[14]

---

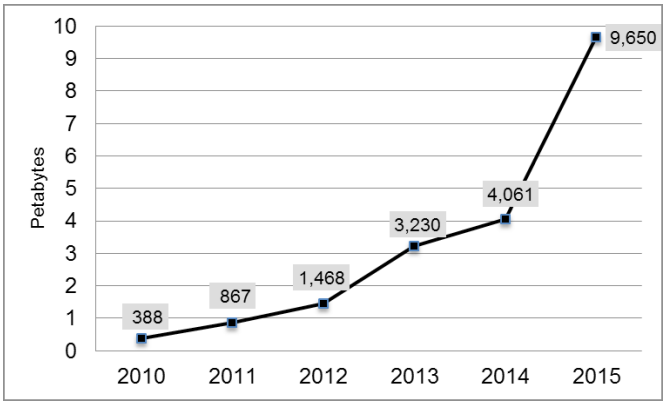
12. CTIA 2015 Survey at 2.

13. Monica Anderson, *6 Facts About Americans and Their Smartphones*, Pew Research Center (Apr. 1, 2015), http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/.

14. *Id.* (noting the following percentages of "smartphone-dependent" Americans: 18-29 year olds (15%); adults with an annual household income of less than $30,000 (13%) versus adults with an income of $75,000 or above (1%); Latinos (13%) and African Americans (12%) versus whites (4%)).

Smartphones allow users to do everything from take and share photos, connect with friends through a variety of video and text-based communication tools, find the fastest route to a new location, stream music, research health information, play games, and track finances—and do all of these things at the same time. As a result, smartphones transmit and receive vast amounts of data. As more Americans have switched to smartphones, the amount of data transferred over wireless networks has increased significantly—2,400% between 2010 and 2015 alone[15] —and service providers have installed more towers to handle that increase.[16]

Chart 3: Wireless Data Traffic (in Petabytes)[17]



15. CTIA 2015 Survey at 8 (388 billion megabytes in 2010, 9,650 billion megabytes in 2015).

16. Blaze Testimony at 10.

17. CTIA 2015 Survey at 8. One source has described a petabyte of data as the equivalent of 20 million four-drawer filing cabinets filled with text. *See* Jesus Diaz, *How Large Is a Petabyte?*, Gizmodo (July 8, 2009), http://gizmodo.com/5309889/how-large-is-a-petabyte.

B. As the Number of Cell Towers and Amount of Data Transmitted Increases, the Location Data Generated by Cell Phones Becomes Increasingly More Detailed

When cell phones connect to cell sites, they generate CSLI—a record of the location of the cell tower the phone connected to at a specific moment in time. Modern cell phones—particularly smartphones—generate vast amounts of CSLI because they routinely send and receive data whenever the phone is on.

Cell phones generate CSLI even in the absence of any user interaction with the phone, in part due to "'applications that continually run in the background that send and receive data (*e.g.*, email applications) without a user having to interact with the cellular telephone.'" *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1014 (N.D. Cal. 2015) ("*2015 N.D. Cal. Opinion*") (quoting Declaration of FBI Special Agent Hector M. Luna). Although some courts have limited their analysis of CSLI to data generated when users place and terminate a call,[18] the government has admitted it seeks access to CSLI generated by apps running in the background. *See id.* at 1033.

Cell phones connect with towers to exchange data on average every seven to nine minutes but can attempt to connect as frequently as every seven seconds.[19] Because

18. *See United States v. Davis*, 785 F.3d 498, 503 (11th Cir. 2015); *see also In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013) ("Fifth Circuit Opinion").

19. *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1028; Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 703 (2011).

these data exchanges create a record of when the user connected to the tower, along with the location of the tower itself, they reveal where the phone—and by proxy, its owner—has travelled. Cell providers store this data for up to five years[20] and can also track CSLI in near real-time.[21]

Law enforcement officers rely on CSLI to place a suspect at a specific location at a specific time, such as at the scene of a crime. *See, e.g.*, *United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2016) (FBI used CSLI to place defendants to within 1/2 to 2 miles of robbery locations at times robberies occurred); *see also United States v. Graham*, 796 F.3d 332, 341 n.11 (4th Cir. 2015) (panel). In the past, CSLI was less accurate, because it consisted only of the location of the base station the phone connected to and the approximate "sector" served by that base station. Sectors could be several miles in diameter, so the phone could, theoretically, be anywhere within that area.

Now, however, CSLI has become much more detailed and specific. As the number of cell towers has increased and cell sites have become more concentrated, the geographic area covered by each cell sector has shrunk.[22] Cell phone triangulation (data from three towers instead of one), allows more precise location tracking, and with newer cell technology, providers can determine not just the location of the cell site the phone connects to, but, by

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

21. *See Tracey v. State,* 152 So. 3d 504, 507 (Fla. 2014).

22. Blaze Testimony at 10.

"correlating the precise time and angle at which a given device's signal arrives at multiple sector base stations," they can determine where the phone is located within a sector.[23] This can shrink accuracy down to within 50 meters.[24] Providers are also using small base stations designed to serve individual homes or offices, or even particular floors of buildings.[25] With these technologies, providers can determine "a phone's latitude and longitude at a level of accuracy that can approach that of GPS."[26]

These advances in cell service technology have especially impacted dense metropolitan areas with large numbers of mobile devices attempting to exchange data. For example, within two miles of the Supreme Court building, there are approximately 130 cell towers and 900 antennae.[27] In areas like these, the higher concentration of towers and antennae allow phones' locations to be pinpointed with even greater accuracy.

---

23. *Id.* at 12.

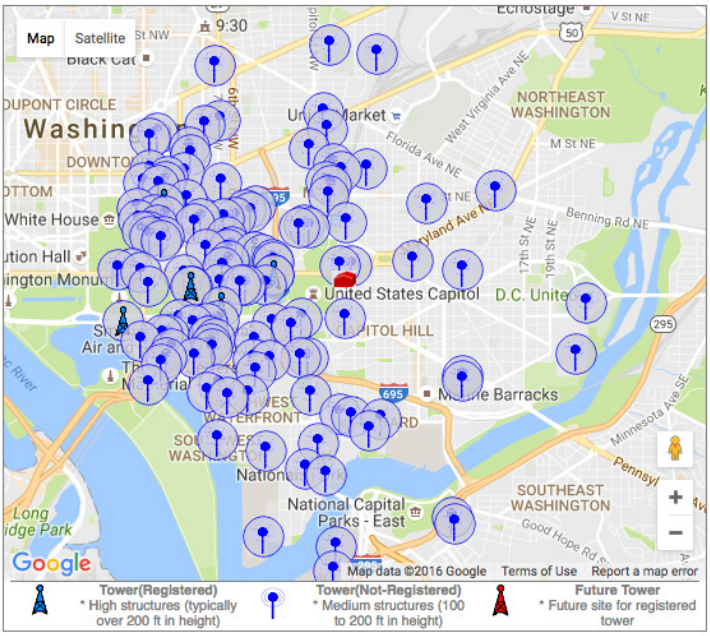
24. *Id.*

25. *Id.* at 11.

26. *Id.* at 12.

27. AntennaSearch.com, http://tinyurl.com/jgawkyp (tower search results); http://tinyurl.com/hkx4t4h (antenna search results).

Map of Cell Towers Within Two Miles of Supreme Court[28]



C. Law Enforcement Routinely Requests Access to Months of CSLI Without a Warrant

As cell phones saturate the country, law enforcement agencies routinely seek access to CSLI in criminal cases. The number of these requests is staggering. For example, AT&T alone received 36,935 requests for CSLI in the first half of 2016 and 76,340 requests in all of 2015.[29] Verizon

28. *Id.*

29. *See* AT&T, *AT&T Transparency Report* 4 (2016), *available at* http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf (disclosing number of

received 24,928 requests in the first half of 2016 and 50,066 requests in 2015.[30] Sprint, the service provider in *Graham*, received 30,640 requests for real-time location data in the first half of 2016 and 64,854 requests in 2015.[31] *Graham*, 796 F.3d at 341 (panel). T-Mobile, the parent company of MetroPCS and the service provider in *Carpenter*, 819 F.3d at 885, does not report requests for CSLI specifically but received far more requests for customer data as a whole than its much larger rivals.[32]

As high as these numbers are, they do not tell the full story. Each request may seek information on many different phones. For example, in *Carpenter*, officers

---

requests for historical CSLI, real-time CSLI, and "cell tower dumps" – identifying information for all phones that connected to a tower during a given period of time).

30. *See* Verizon, *Verizon's Transparency Report for the First Half of 2016: U.S. Report* (2016), *available at* https://www.verizon.com/about/portal/transparency-report/us-report/; *see also* Verizon, *2015 (1st Half) Transparency Report* and Verizon, *2015 (2nd Half) Transparency Report*, *available at* https://www.verizon.com/about/portal/transparency-report/archive/ (numbers include "location information" and cell tower dumps).

31. Sprint, *Sprint Corporation Transparency Report* 4 (July 2016), *available at* http://goodworks.sprint.com/content/1022/files/Transaparency%20Report%20July2016.pdf (Sprint's report does not track other forms of location data).

32. Abigail Tracy, *T-Mobile Leads US Wireless Carriers In Government Data Requests*, Forbes (July 6, 2015), http://www.forbes.com/sites/abigailtracy/2015/07/06/t-mobile-leads-u-s-wireless-carriers-in-government-data-requests/#5cb644f54c88; *see also* T-Mobile, *T-Mobile Transparency Report* (2013-2014), *available at* https://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf.

relied on three requests to access information about 16 different phones. 819 F.3d at 884. The quantity of data requested for each phone may vary as well. In *Graham*, with a single request, agents were able to obtain 221 days worth of location information for Mr. Graham and his co-defendant. 796 F.3d at 341 (panel). In *Carpenter*, the FBI obtained three to four months worth of data. 819 F.3d at 895 (Stranch, J., concurring).

The majority of these demands for CSLI are warrantless. Verizon has reported that two-thirds of all law enforcement requests for historical and real-time location information were made via a court order,[33] like the orders issued under 18 U.S.C. § 2703(d) that the government obtained in both *Carpenter* and *Graham*. *Carpenter*, 819 F.3d at 884; *Graham*, 796 F.3d at 344 (panel).

II. CSLI Paints a Revealing Portrait of a Person's Movements, Presenting Even Greater Privacy Concerns Than the GPS Tracker at Issue in *Jones*

The amount of CSLI generated as a result of society's reliance on cell phones means that law enforcement has access to an incredibly detailed picture of people's private lives and associations. *Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring). As noted in one of the first published opinions to address CSLI, the "combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year." *In re*

33. *See* Verizon, *Verizon United States Report* (2016), *available at* https://www.verizon.com/about/portal/transparency-report/?page_id=2133.

Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) ("*S.D. Tex. 2005 Opinion*").

Until the twenty-first century, "society'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." *Jones*, 132 S.Ct. at 964 (Alito, J., concurring in the judgment). But CSLI has eviscerated that expectation and presents even greater privacy concerns than the GPS device this Court considered in *Jones*.

First, a GPS device attached to a car can only go where the car goes, while a cell phone goes everywhere its owner goes. As this Court noted in *Riley*, "three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting they even use their phones in the shower." 134 S.Ct. at 2490 (citations omitted). Therefore, as the panel noted in *Graham*, "unlike GPS monitoring of a vehicle, examination of historical CSLI can permit the government to track a person's movements between public and private spaces, impacting at once her interests in both the privacy of her movements and the privacy of her home." 796 F.3d at 348 (panel). And, in fact, using Mr. Graham's records, the ACLU was able to infer details about his patterns of movement, including when he and his pregnant wife visited her obstetrician, when he traveled to or from his home, and nights he spent away from home.[34]

34. *See* Bennett Stein, *Fighting a Striking Case of Warrantless Cell Phone Tracking*, ACLU (July 1, 2013), https://www.aclu.

Second, CSLI can give law enforcement far more information about a person's movements than the 28 days of monitoring that five members of this Court found problematic in *Jones*. *See* 132 S.Ct. at 964 (Alito, J., concurring in the judgment) (line at which tracking of vehicle became a search "was surely crossed before the 4–week mark"); *id.* at 955 (Sotomayor, J., concurring). The government obtained 88 days and 127 days worth of location information for each defendant in *Carpenter* and 221 days of data for each defendant in *Graham*. *Carpenter*, 819 F.3d at 886; *Graham*, 796 F.3d at 349 (panel). In other cases, the government has sought records for 67 days, 113 days, and 180 days. *Davis*, 785 F.3d at 501; *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F.Supp.2d 113, 114 (E.D.N.Y. 2011) ("*2011 E.D.N.Y. Opinion*"); *United States v. Jones*, 908 F.Supp.2d 203, 206 (D.D.C. 2012). Because cell providers keep records of CSLI for up to five years, law enforcement officers could seek access to this data for even longer periods of time. Such extensive monitoring reveals a wealth of information about a person's expressive and associational activities protected by the First Amendment, in addition to the Fourth Amendment's protections against unreasonable searches. *See Smith*, 442 U.S. at 751 (Marshall, J. dissenting) (citing *NAACP v. Alabama*, 357 U.S. 449, 461 (1958)); *Roberts v. U.S. Jaycees*, 468 U.S. 609, 617-18 (1984).

Third, historical CSLI allows police to reconstruct a person's *past* movements. As Justice Alito noted in

---

org/blog/fighting-striking-case-warrantless-cell-phone-tracking (noting records were analyzed with Mr. Graham's "assistance and permission").

Jones, tracking a car's location for 28 days "would have [traditionally] required a large team of agents, multiple vehicles, and perhaps aerial assistance." 132 S.Ct. at 963 (Alito, J., concurring in the judgment). But CSLI allows police to go back in time to recreate a person's past movements, something not possible with the GPS tracker in *Jones* and *never* available through traditional law enforcement investigative techniques. *See Commonwealth v. Augustine*, 4 N.E.3d 846, 865 (Mass. 2014).

Finally, CSLI is generated for *all* phones, not simply those under investigation. Accordingly, unlike the GPS device in *Jones*, police need not even know in advance whether they want to track a particular individual. Rather, they have the ability to track nearly *any* person's location.

This Court has noted it is "foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001). With historical CSLI, the "practical" privacy protections of tracking a person's movement for months in the "pre-computer age"—namely difficulty and cost—have faded away. *Jones*, 132 S.Ct. at 963 (Alito, J., concurring in the judgment).

III. Courts Have Misapplied *Smith v. Maryland* to Bar Fourth Amendment Protection for CSLI

The majority opinions in *Carpenter* and *Graham* relied on this Court's decision in *Smith v. Maryland* to hold that the Fourth Amendment does not protect CSLI. *Smith* held that an individual has no reasonable expectation of privacy in the telephone numbers he dials because they

are business records that he "voluntarily conveyed" to the phone company. 442 U.S. at 744. But as other state and federal courts and judges have noted, *Smith* should not control here. Given "the important constitutional issues presented and the conflicting results reached" in CSLI cases, this Court should grant *certiorari* to clarify the scope of its prior rulings on the expectation of privacy in information shared with third parties. *Heffron v. International Society for Krishna Consciousness,* 452 U.S. 640, 646 (1981).

A. Courts and Judges Disagree on the Application of the "Third-Party Doctrine" to CSLI

In the roughly ten years that courts have been considering the Fourth Amendment's application to CSLI, there has been intense disagreement among judges and courts in both the state and federal systems. Within the five federal Circuit Courts of Appeal that have addressed the issue, many judges would hold or have held the third-party doctrine does not bar Fourth Amendment protection for CSLI.[35] In federal circuits where appellate courts have yet to address this issue—including the Second, Seventh, and Ninth Circuits—district court judges have also held

35. *See, e.g.*, *United States v. Graham*, 824 F.3d 421, 446 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in part, joined by Floyd, J. and Thacker, J.); *Graham*, 796 F.3d at 354 (panel) (Davis, J., joined by Thacker, J.); *Carpenter*, 819 F.3d at 895 (Stranch, J., concurring); *Davis*, 785 F.3d at 535 (Martin, J., joined by Pryor, J., dissenting); *United States v. Davis*, 754 F.3d 1205, 1217 (11th Cir. 2014) (panel); *Fifth Circuit Opinion*, 724 F.3d at 615–16 (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, 317–18 (3d Cir. 2010) ("*Third Circuit Opinion*").

the third-party doctrine does not apply to CSLI.[36] Other federal judges have recognized the strong privacy interest in CSLI but concluded their hands were tied by *Smith*,[37] or simply acknowledged the need for further guidance from this Court.[38] As one court concluded after reviewing 87 CSLI opinions, "these decisions are impossible to reconcile." *In Matter of United States*, 40 F. Supp. 3d 89, 91 (D.D.C. 2014).

Graham and *Carpenter* are also in conflict with several state supreme court decisions, another factor weighing in favor of granting certiorari. *See Turner v. Rogers,* 131 S.Ct. 2507, 2514 (2011). The supreme courts of three states—New Jersey, Massachusetts, and Florida—have held that law enforcement needs a warrant to access at least some types of CSLI. *See Tracey,* 152 So. 3d 504 (Fla. 2014); *Augustine*, 4 N.E.3d 846 (Mass. 2014)

---

36. *See, e.g., 2011 E.D.N.Y. Opinion*, 809 F. Supp. 2d at 126; *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294, 322-23 (E.D.N.Y. 2005); *In re Application of U.S.*, Nos. 1:06–MC–6, 1:06–MC–7, 2006 WL 1876847, at *4 (N.D. Ind. July 5, 2006); *U.S. v. Alvarez*, No. 14-CR-00120-EMC, 2016 WL 3163005 *at 3 (N.D. Cal. June 3, 2016); *U.S. v. Cooper*, No. 13–693, 2015 WL 881578, at *7-8 (N.D. Cal. Mar. 2, 2015); *N.D. Cal. 2015 Opinion*, 119 F. Supp. 3d at 1027.

37. *See, e.g., United States v. Graham*, 846 F. Supp. 2d 384, 389–90, 394 (D. Md. 2012), *aff'd but criticized,* 796 F.3d 332 (4th Cir. 2015), *adhered to in part on reh'g en banc,* 824 F.3d 421 (4th Cir. 2016); *Davis*, 785 F.3d at 524 (Rosenbaum, J. concurring); *In re Application of U.S.*, 736 F. Supp. 2d 578, 589, n.12 (E.D.N.Y. 2010), rev'd (Nov. 29, 2010).

38. *See, e.g., United States v. Thomas*, No. 3:15CR80, 2015 WL 5999313, at *7 (E.D. Va. Oct. 13, 2015).

(deciding case under the state constitution); *State v. Earls*, 70 A.3d 630 (N.J. 2013) (same). As the Florida Supreme Court recognized, "cumulative cell-site-location records implicate sufficiently serious protected privacy concerns" and cell-phone users have a reasonable expectation of privacy in these records, despite the fact that they are collected and stored by a third party. *Tracey*, 152 So. 3d at 523 (citing *2011 E.D.N.Y. Opinion*, 809 F. Supp. 2d at 126). Although *Tracey* addressed real-time CSLI tracking, its Fourth Amendment analysis could be applied to historical CSLI as well—putting its decision in direct conflict with *Davis* and thus subjecting Florida residents to differing standards depending on whether a state or federal court authorizes an investigation. *See id.* (concluding same principle applies to historical and real-time CSLI).

As the dissenting judges noted in *Graham*, the majority holdings in *Graham* and *Carpenter*, "under the guise of humble service to Supreme Court precedent, markedly advance[] the frontlines of the third-party doctrine." *Graham*, 824 F.3d at 449 (en banc) (Wynn, J., dissenting). Given the broad disagreement over the proper application of the third-party doctrine, it is time for this Court to further "assess[] the application of the Fourth Amendment in the context of new technology." *Carpenter*, 819 F.3d at 897 (Stranch, J., concurring).

B. Users Do Not "Voluntarily Convey" CSLI to Providers

The judges and courts finding *Smith* does not apply to CSLI have the better argument. *Smith* rests on the holding that individuals knowingly and voluntarily convey the telephone numbers they dial to a third party. 442

U.S. at 744. But unlike when someone affirmatively dials a specific number, cell phone users do not knowingly—let alone voluntarily—transmit location data to cell providers. *See Augustine*, 4 N.E.3d at 862. It is "unlikely that cell phone customers are [even] aware that their cell phone providers collect and store historical location information." *Third Circuit Opinion*, 620 F.3d at 317. Instead, CLSI is "transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge." *S.D. Tex. 2005 Opinion*, 396 F. Supp. 2d at 756–57.

As described above, phones generate CSLI whenever they are on and searching for a signal. CSLI includes data generated when users make calls, but this data is dwarfed by the data "generated by *passive* activities such as automatic pinging, continuously running applications ("apps"), and the receipt of calls and text messages." *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1024 (internal quotations and citation omitted). Further, such records may be stored and turned over to the government "by any number of cellular service providers other than the cell phone user's[.]" *Id.* at 1033.

The vast majority of CSLI generated by modern cell phones is thus created "with far less intent, awareness, or affirmative conduct on the part of the user than what was at issue in . . . *Smith.*" *Id.* at 1029. Such passive, unknowing generation of CSLI does not amount to a "voluntary conveyance" under the third-party doctrine. *Id.*; *see also Davis*, 785 F.3d at 534 (Martin, J., dissenting); *Tracey*, 152 So. 3d at 525–26.

Some courts have held that merely choosing to carry and turn on a phone is sufficient to meet *Smith's* voluntary conveyance test. *See, e.g.*, *Graham*, 824 F.3d at 428 (en banc); *Carpenter*, 819 F.3d at 888. But when a phone can be considered a "feature of human anatomy," owning and carrying a phone is hardly a choice at all. *Riley*, 134 S.Ct. at 2484; *see also City of Ontario v. Quon*, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."). As the New Jersey Supreme Court recognized, "cell-phone users have no choice but to reveal certain information to their cellular provider," but "no one buys a cell phone to share detailed information about their whereabouts with the police." *Earls*, 214 N.J. at 584, 587.

C. The Fourth Amendment Protects Sensitive Information Even if People Know a Third Party May Access It

Smith did not create a blanket rule that all information shared with a third party is denied Fourth Amendment protection. Even if users somehow "voluntarily" convey CSLI to cell providers, this Court's decisions make clear that the fact that such highly sensitive information is held by a third party does not automatically defeat an individual's expectation of privacy. *See, e.g.*, *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (patient has reasonable expectation of privacy in diagnostic test results held by hospital); *Bond v. United States*, 529 U.S. 334, 338–39 (2000) (passenger retained expectation of privacy in luggage placed in bus overhead bin despite possibility of external inspection by others); *Stoner v.*

California, 376 U.S. 483, 489–90 (1963) (hotel guests entitled to constitutional protection even though they provide "implied or express permission" for third parties to access their rooms).

In *Smith* itself, the Court cautioned that a "normative inquiry" might be necessary when individuals' subjective expectation of privacy is inconsistent with "well-recognized Fourth Amendment freedoms." 442 U.S. at 740 n.5. In other words, the Fourth Amendment may still protect CSLI even if individuals voluntarily convey their location to cell providers and know that the government may seek this information from these companies.

D. Americans Reasonably Expect Location Data to Remain Private

A "normative inquiry" shows that, contrary to the conclusion reached in *Graham* and *Carpenter*, the public believes location information stored on and generated by mobile phones is private and that this expectation is reasonable. *See Oliver v. United States*, 466 U.S. 170, 178 (1984) (noting that one factor the Court uses to assess "the degree to which a search infringes upon individual privacy" is the "societal understanding that certain areas deserve the most scrupulous protection from government invasion"). When it comes to new technologies, "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior." *Quon*, 560 U.S. at 759.

Recent studies show Americans expect privacy in their cell phones, especially when it comes to location

information. In 2014, the Pew Research Center reported that 82% of Americans consider the details of their physical location over time to be sensitive information—more sensitive than their relationship history, religious or political views, or the content of their text messages.[39] In 2012, another study found that cell phone owners take steps to protect their personal information and mobile data, and more than half of smartphone owners have uninstalled or decided to not install an app due to privacy concerns.[40] In addition, more than 30% of smartphone owners polled took affirmative steps to safeguard their privacy: 19% turned off location tracking on their phones, which disables location tracking for certain apps but does not prevent the service provider from logging CSLI.[41] The numbers are higher for teenagers, with Pew reporting 46% of teenagers turned location services off.[42] A 2013 survey conducted on behalf of Internet company TRUSTe found 69% of American smartphone users were concerned

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

40. Jan Lauren Boyles, *et al.*, *Privacy and Data Management on Mobile Devices*, Pew Research Internet & American Life Project (Sept. 5, 2012) *available at* http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.

41. *Id.*

42. Kathryn Zickuhr, *Location-Based Services*, Pew Research Internet & American Life Project (Sept. 12, 2013) http://www.pewinternet.org/2013/09/12/location-based-services/.

about being tracked.[43] And a 2009 Carnegie Mellon survey of perceptions about location-sharing technologies showed that, on average, participants believed the risks of location-sharing technologies outweighed the benefits and were "extremely concerned" about controlling access to their location information.[44]

As noted above in Section III.A, federal and state courts have both supported the idea that it is objectively reasonable to find historical CSLI private and required the government to use a probable cause search warrant to obtain this sensitive data. Although other courts, like *Graham* and *Carpenter*, have reached the opposite conclusion, the fact that reasonable jurists have—and continue to—disagree undermines the conclusion reached in both cases that an expectation of privacy in CSLI is unreasonable.

---

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

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

CONCLUSION

Given the prevalence of cell phones and the quantity of law enforcement requests for this sensitive information, *Graham* and *Carpenter* present questions of compelling national importance. The legal protections offered for CSLI are not uniform, and courts have issued conflicting opinions on the issue, leaving the public and law enforcement in limbo.

This Court should therefore grant *certiorari* in both *Graham* and *Carpenter* to resolve the issue, provide clear guidance to both the public and law enforcement, and ultimately conclude these sensitive records are protected by the Fourth Amendment's warrant requirement.

Dated: October 25, 2016

Respectfully submitted,

Rachel Levinson-Waldman
Michael W. Price
Brennan Center for Justice
at NYU School of Law
161 Avenue of the Americas,
12th Floor
New York, New York 10013
(646) 292-8335

Jennifer Lynch
Counsel of Record
Andrew Crocker
Jamie Williams
Stephanie Lacambra
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
jlynch@eff.org

Attorneys for Amici Curiae

APPENDIX

APPENDIX

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society. EFF has served as *amicus* in Fourth Amendment cases before this Court, including in *City of Los Angeles v. Patel*, 135 S.Ct. 2443 (2015), *Riley v. California*, 134 S.Ct. 2473 (2014), *Maryland v. King*, 133 S.Ct. 1958 (2013), *United States v. Jones*, 132 S.Ct. 945 (2012), and *City of Ontario v. Quon*, 560 U.S. 746 (2010). EFF has also served as amicus in numerous cases addressing Fourth Amendment protections for CSLI, including, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015); *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015); and *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016).

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice. The Center's Liberty and National Security ("LNS") Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic

intelligence gathering policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms. As part of its work in this area, the Center has filed numerous *amicus* briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *Riley v. California*, 134 S.Ct. 2473 (2014); *United States v. Jones*, 132 S.Ct. 945 (2012); *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *petition for cert. docketed*, No. 16-402 (Sept. 28, 2016); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016), *petition for cert. docketed*, No. 16-263 (Aug. 30, 2016); *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197 (2d Cir. 2016), *petition for reh'g* en banc *filed*, No. 14-2985 (Oct. 17, 2016); *United States v. Moalin*, No. 13-50572 (9th Cir. filed Nov. 5 1015); and *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015).

The Center for Democracy & Technology ("CDT") is a nonprofit public interest group that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized Internet. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of Internet users. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The Constitution Project ("TCP") is a constitutional watchdog that brings together legal and policy experts from across the political spectrum to promote and defend

constitutional safeguards. TCP's bipartisan Liberty and Security Committee, founded in the aftermath of September 11th, is composed of policy experts, legal scholars, and former high-ranking government officials from all three branches of government. This diverse group makes policy recommendations to protect both national security and civil liberties, for programs ranging from government surveillance to U.S. detention. Based upon their reports and recommendations, TCP files amicus briefs in litigation related to these issues. TCP is dedicated to ensuring that transformative changes in technology do not undermine the privacy rights that the Framers enshrined in our Constitution. For example, TCP's Liberty and Security Committee has published reports on public video surveillance systems (analyzing how rapid technological advances have eroded the distinction between private and public spaces in the context of such systems) and location tracking (finding that the Fourth Amendment requires law enforcement to obtain a warrant before employing GPS technology to conduct prolonged tracking of an individual's movements, even if on public streets).

The National Coalition to Protect Civil Freedoms ("NCPCF") is a coalition of 18 organizations (about half Muslim and half non-Muslim) dedicated to the preservation of our civil freedoms, particularly in the so-called War on Terror. NCPCF focuses on three areas in which civil rights have significantly eroded since 9/11: Prevention of discrimination and Islamophobia; prevention of abuse of prisoners; and prevention of preemptive prosecutions (defined as the use of pretext charges, unfair

sting operations, and generally prosecutions based on governmental suspicion of the target's ideology)

NCPCF represents the interests of Muslims and others targeted by government surveillance (which often leads to pressure to become an informant or other improper measures) based on their religion, race, country of origin, or ideology.