No. 15-146

IN THE

Supreme Court of the United States

QUARTAVIOUS DAVIS,

Petitioner,

v.

UNITED STATES,

Respondent.

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

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW, CENTER FOR DEMOCRACY & TECHNOLOGY, THE CONSTITUTION PROJECT AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF PETITIONER

JEFFREY T. GREEN
Co-Chair, Amicus Committee
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1660 L Street, NW
Washington, DC 20036
(202) 872-8600

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

HANNI M. FAKHOURY
Counsel of Record
JENNIFER LYNCH
ANDREW CROCKER
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
hanni@eff.org

Counsel for Amici Curiae

260927

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

TABLE OF CITED AUTHORITIES

Page

FEDERAL CASES

Cited Authorities

Cited Authorities

Cited Authorities

Cited Authorities

Cited Authorities

Page

STATEMENT OF INTEREST[1]

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).

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

1. Pursuant to Supreme Court Rule 37.2(a), *amici* have provided timely notice to all counsel, and both parties consented 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.

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*, 2014 WL 943094 (E.D. Mich. 2014), *appeal docketed*, No. 14-1805 (6th Cir. Jun. 24, 2014); *United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014), *rehearing* en banc *granted*, 791 F.3d 290 (Mem.) (Jun. 29, 2015); *In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation*, 15 F.Supp.3d 466 (S.D.N.Y. 2014), *appeal docketed*, No. 14-2985-cv (2d Cir. Aug. 12, 2014); *Amnesty International USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011); *Hepting v. AT&T Corp.*, 539 F.3d 1157 (9th Cir. 2008); and *In re Nat'l Sec. Agency Telecommunications Records Litigation*, 564 F.Supp.2d 1109 (N.D. Cal. 2008). This brief does not purport to represent the position of NYU School of Law.

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 Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of approximately 10,000 direct members in 28 countries, and 90 state, provincial and local affiliate organizations totaling up to 40,000 attorneys. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL files numerous *amicus* briefs each year in this Court and other courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system

as a whole. NACDL has frequently appeared as *amicus curiae* before this Court in furtherance of its mission to safeguard fundamental constitutional rights.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

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 different types of private information—potentially the "sum of an individual's private life"—makes the data available from a cell phone so qualitatively and quantitatively different from its analog counterparts as to require a warrant prior to search. *Riley*, 134 S.Ct. at 2489.

However, the private data available from a cell phone 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 phone tower. Every time it does this, it generates a small piece of information, stored by the phone company, about which tower the phone connected to—essentially where the phone was—on a given time and date. These small bits of data—called cell site location information (CSLI)—are aggregated by phone companies over time 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).

Cell site location information is proving to be increasingly useful to law enforcement officers. As cell phone usage has increased, so too have the number of cell towers or cell "sites," meaning this data is growing more and more precise every year. Equipped with CSLI, police can now not only locate criminal suspects on the run or pinpoint defendants to specific crime scenes, but can also reconstruct a person's movements for many days in the past—from 67 days in this case to 221 days in *United States v. Graham*, ___ F.3d ___, 2015 WL 4637931, *3 (4th Cir. Aug. 5, 2015).

The petition for *certiorari* asks this Court to address whether the Fourth Amendment prohibits the warrantless seizure and search of these records. This is a question of national importance as federal and state courts across the country answer it in conflicting ways. The *en banc* Eleventh Circuit Court of Appeals in this case found no expectation of privacy in these records, meaning law enforcement in Georgia (as well as Alabama and Florida) do not need a warrant to access them. *United States v. Davis*, 785 F.3d 498, 511 (11th Cir. 2015) (*en banc*). But for law enforcement in Georgia's northern neighbor South Carolina (as well as Maryland, North Carolina, Virginia and West Virginia), the Fourth Circuit Court of Appeals has reached the opposite conclusion, finding an expectation of privacy in these records and requiring law enforcement to use a warrant to obtain them. *Graham*, 2015 WL 4637931, at *8.

This confusion not only means the public is left with differing legal protection under federal law, but also

creates a risk of uncertainty for law enforcement. As cell phone location information becomes more precise and revealing, and as law enforcement increasingly relies on this data to secure criminal convictions, this Court should grant *certiorari* to resolve this split of opinion and make clear that *all* Americans have an expectation of privacy in their cell site location information under the Fourth Amendment.

ARGUMENT[2]

The dramatic increase over just a few years in the number of cell phones and cell sites and the amount of data they generate, combined with the clear increase in law enforcement demands for this data, shows that it is time for this Court to address the Fourth Amendment privacy implications of CSLI. The current Circuit split only underscores this point. *Compare Graham*, 2015 WL 4637931, at *8 (warrant required to obtain historical CSLI) *with Davis*, 785 F.3d at 511 *and In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013) (warrant not required to obtain historical CSLI).

A. The Number of Cell Phones and Cell Sites Has Dramatically Increased in the Last Twenty 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. In 2015, owning a cell phone is not a luxury; today more

2. All Web sites cited in this brief were last visited on August 25, 2015.

than 90%[3] of all American adults have a cell phone, and landline phones are becoming obsolete.[4] Since 1986, the year Congress enacted the Stored Communications Act ("SCA"), the number of cell phones in the United States has increased by 52,000%. Today, there are an estimated 355 million cell phone accounts[5] in the United States, meaning there are 34 million more cell phone accounts than people in the United States.[6]

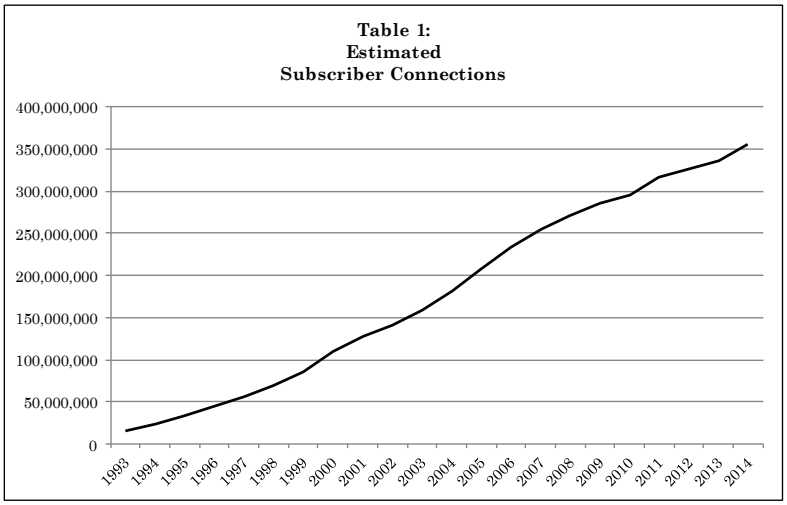
---

3. Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, Pew Research Center, Jun. 6, 2013, http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

4. *See* Steven Shepard, "Americans Continue to Drop Their Landline Phones," *National Journal*, Dec. 18, 2013, http://www.nationaljournal.com/hotline-on-call/americans-continue-to-drop-their-landline-phones-20131218 (citing Centers for Disease Control and Prevention statistics finding 36.5% of U.S. adults live in household with no landline phone).

5. Table 1 was 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 – The Wireless Association Annual Wireless Industry Survey, at p. 3, *available at* http://www.ctia.org/docs/default-source/Facts-Stats/ctia_survey_ye_2014_graphics.pdf?sfvrsn=2.

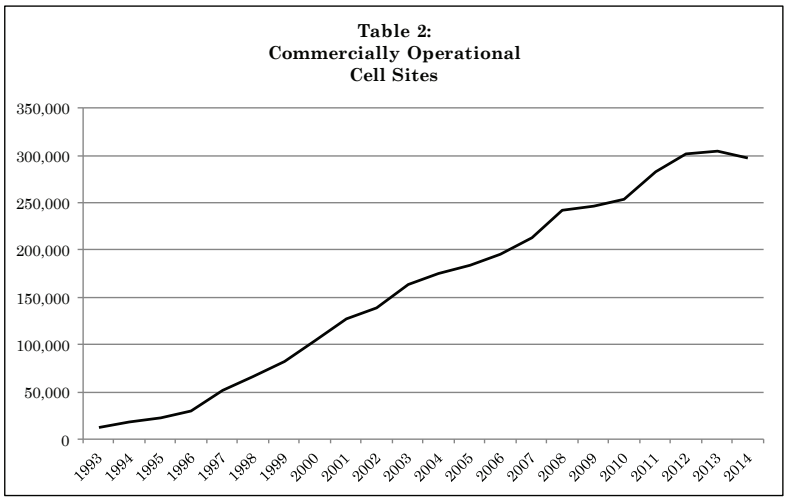
6. According to the United States Census Bureau, the population of the United States as of August 25, 2015 was approximately 321,601,275. *See* U.S. and World Population Clock, United States Census Bureau, http://www.census.gov/popclock/.



Cell phones work by sending a radio signal from the handset or phone a user holds in their hand to a network of radio base stations known as cell towers. These towers typically face three or four different directions, and each of these individual sides to the tower are known as a cell "site" or "sector." These sectors contain antennas that detect the radio signal emanating from a cell phone and connect the phone to the cellular network.[7] As cell phone usage has increased, so too has the number of cell phone

7. *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 (2013) (written testimony of Professor Matt Blaze, University of Pennsylvania), *available at* 2013 WL 1771788 (Apr. 25, 2012).

towers and cell sites needed to handle the increased cell phone traffic.[8]



The increase in cell sites is not due solely to the increase in the number of cell phones in the United States, but also to the sharp increase in wireless data traffic over the last few years.[9] As cell phones have eliminated the need for a landline telephone, smartphones—"minicomputers that also happen to have the capacity to be used as a

8. Table 2, like Table 1, was also generated using statistics from the CTIA – The Wireless Association Annual Wireless Industry Survey. *See* http://www.ctia.org/docs/default-source/Facts-Stats/ctia_survey_ye_2014_graphics.pdf?sfvrsn=2 at p. 10.

9. Wireless data traffic has increased 26% year-over-year since 2010. CTIA – The Wireless Association Annual Wireless Industry Survey, *available at* http://www.ctia.org/docs/default-source/Facts-Stats/ctia_survey_ye_2014_graphics.pdf?sfvrsn=2 at p. 8.

telephone," *Riley*, 134 S.Ct. at 2489—have taken over the mobile phone market. In 2011, 35% of American adults owned a smartphone. Today, that number is 64%.[10] As more and more Americans switch to Internet-enabled smartphones, the data transferred over wireless networks has increased and required cell phone service providers to install more and more cell sites to handle the load. Naturally, that means phones are generating an increasing amount of CSLI.

B. Cell Site Location Information Paints a Revealing Portrait of a Person's Movements.

Cell site location information is a record police can obtain from a cell phone service provider of which cell phone tower a phone connects to at a specific moment. As explained above, modern cell phones—particularly smartphones—generate an incredible amount of CSLI because they routinely send and receive data via cell sites, even in the absence of any user interaction with the phone. Because these data exchanges create a record of the time and date when the user connected to the tower, along with the location of the tower itself, this data reveals where the phone—and by proxy, its owner—has travelled throughout her daily life.

As smartphone users increasingly multitask on their phones—for example, uploading a picture to a social media site, then switching to an email program to send a work-

10. 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/.

related message or read a news story on the Internet, all while listening to music from a streaming music service—the phone is constantly exchanging data with cell sites and generating a staggering amount of CSLI.[11]

The Eleventh Circuit below, like other earlier cases, only considered historical cell site data generated when Mr. Davis made and received calls. *See Davis*, 785 F.3d at 503; *see also In re Application of the U.S.*, 724 F.3d at 615 (considering cell site data generated when a "user places and terminates a call."). But the reality is that cell phone users increasingly do not need to actively do anything on their phone to generate CSLI.

As an FBI agent explained in a recent affidavit submitted to a district court considering this very issue, CSLI may be generated by "'applications that continually run in the background that send and receive data (*e.g.*, email applications).'" *In re Application for Tel. Info. Needed for a Criminal Investigation*, ___ F.Supp.3d ___, 2015 WL 4594558, at *13 (N.D. Cal. Jul. 29, 2015) (quoting Declaration of FBI Special Agent Hector M. Luna). The government has admitted it does in fact seek access to location information generated by apps running

11. Modern smartphones are designed to run these various programs (called "apps") continually in the "background" even while the user is not using the program. *See, e.g.,* "Understanding multitasking and background activity on your iPhone, iPad, or iPod touch," *available at* https://support.apple.com/en-us/HT202070 ("Some apps can continue to run in the background. You can allow these apps to refresh themselves by turning on Background App Refresh. This settings lets apps check for new content and download updates, or retrieve updated content in the background when they receive push notifications.").

in the background, a sign of the growing body of sensitive location information available to law enforcement. *See id.* (noting government's 18 U.S.C. § 2703(d) application sought location information generated by apps running in the background).

The amount of CSLI generated as a result of society's reliance on cell phones means that law enforcement has access to an increasingly "precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring). 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. But people keep their cell phones close to them; 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." *Riley*, 134 S.Ct. at 2490 (citing Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013)).[12] Therefore, "unlike GPS monitoring

12. *Available at* http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf at p. 2-3.

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." *Graham*, 2015 WL 4637931, at *11.

Second, cell site location information gives law enforcement an extensive amount of information about a person's movements, far beyond 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) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark."). Here, the government obtained 67 days worth of Mr. Davis' location information. *Davis*, 785 F.3d at 501. In other cases, the government has sought records for 113 days,[13] 180 days,[14] and 221 days.[15] In *Graham*, the case where the government obtained 221 days worth of data, this totaled 29,659 location data points for one defendant and 28,410 data points for the other—"amounting to well over 100 data points for each Appellant per day on average." *Graham*, 2015 WL 4637931, at *12. As cell phone companies keep records of cell site location information for up to five years, it is possible that law enforcement officers could seek access to data for even longer periods

13. *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).

14. *United States v. Jones*, 908 F.Supp.2d 203, 206 (D.D.C. 2012).

15. *Graham*, 2015 WL 4637931, at *3.

of time.[16] This not only implicates the Fourth Amendment's guarantee against unreasonable searches; such extensive monitoring also reveals a wealth of information about a person's expressive and associational activities protected by the First Amendment. *See Roberts v. U.S. Jaycees*, 468 U.S. 609, 617-18 (1984); *NAACP v. Alabama*, 357 U.S. 449, 461 (1958).

Third, historical cell site location information allows police to reconstruct a person's *past* movements. As Justice Alito noted in *Jones*, tracking a car's location over an extended period of time "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." *Jones*, 132 S.Ct. at 963 (Alito, J., concurring in the judgment). But cell site location information allows police to go back in time—potentially as far back as five years if a user is an AT&T customer—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 ones under investigation by law enforcement. Accordingly,

---

16. AT&T keeps historical cell tower location records for five years. *See* October 3, 2013 Letter from Timothy McKone, AT&T Executive Vice President, Federal Relations to U.S. Senator Edward Markey (D-Mass.), at p. 3, *available at* http://www.markey.senate.gov/documents/2013-10-03_ATT_re_Carrier.pdf. Verizon, on the other hand, generally retains such records for one year. *See* October 3, 2013 Letter from William Petersen, Verizon Wireless General Counsel to U.S. Senator Edward Markey (D-Mass.), at p. 3, *available at* https://www.markey.senate.gov/documents/2013-12-09_VZ_CarrierResponse.pdf

unlike the use of a GPS device to track a car, police will never need to know in advance whether they want to track a particular individual. Rather, they will always have the ability to track any person's location.

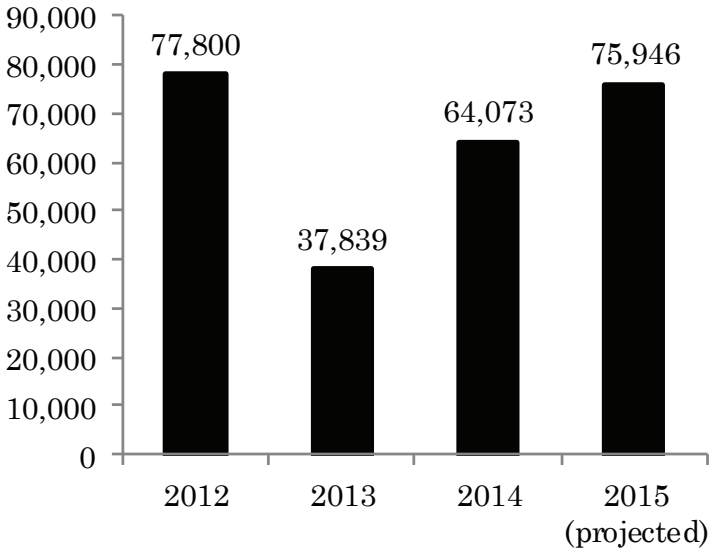
This Court has noted it is "foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001). With historical cell site location information, the "practical" privacy 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).

C. The Number of Law Enforcement Requests for Location Information—Requests Predominantly Made Without a Warrant—Is Increasing.

Unsurprisingly, as cell phones have saturated the United States, the number of law enforcement demands for location information has also increased. For example, after receiving more than 77,800 requests for location information in 2012, AT&T saw a 50% drop for requests the following year. But in just two years, AT&T is about to get back to that peak, and it is on track to receive twice as many law enforcement requests for cell phone location information in 2015 as it received in 2013.[17]

17. The number of requests in Table 3 is for all forms of location data, including historical cell site location records, real time cell site location records and tower dumps, reported by AT&T in its semi-annual Transparency Reports. *See* AT&T Transparency Report, *available at* http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html. The projection

Table 3:
AT&T Location Info Demands

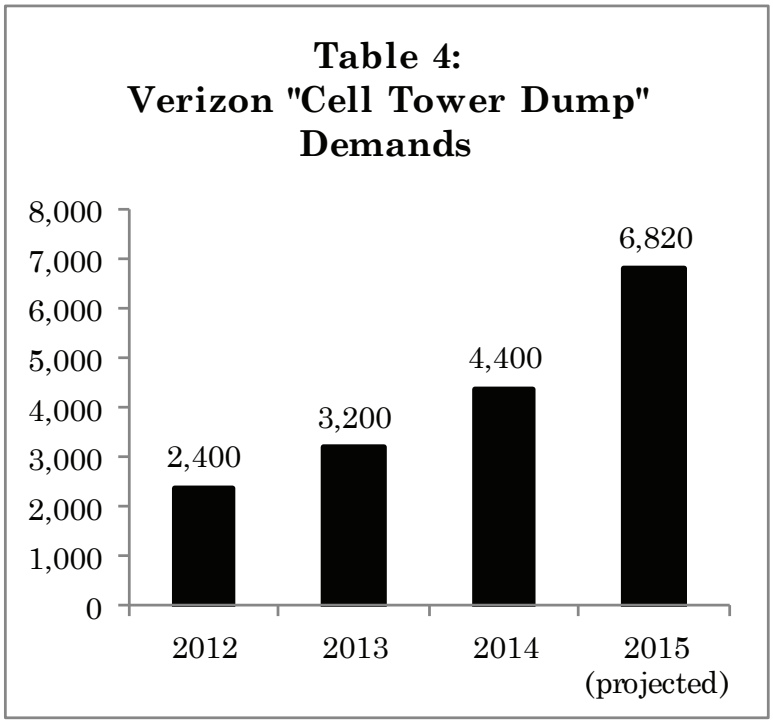


Verizon, the country's largest cell phone service provider, is on track to receive more than twice as many law enforcement requests for a "cell tower dump"—a request to identify all the phone numbers that connected to a specific cell tower during a particular time frame—in 2015 as it did in each of the last three years.[18]

---

for 2015 was determined by doubling the number of requests AT&T reported it received for location information in the first half of 2015. *See* AT&T July 2015 "Transparency Report," at p. 4, *available at* http://about.att.com/content/dam/csr/Transparency%20Reports/Transparency/ATT_Transparency%20Report_July%202015.pdf.

18. Like Table 3, the statistics reported in Table 4 come from Verizon's semi-annual transparency report. *See* http://



Requests for location information are becoming an increasingly larger percentage of the total number of demands AT&T and Verizon are receiving in the context of criminal investigations. In the first half of 2015, location demands were 16% of all the law enforcement demands for user information received by Verizon, up 5% from the previous three years.[19] Similarly, 28% of all demands for

transparency.verizon.com/. The projected number of "cell tower dumps" in 2015 likewise comes from doubling the number of requests Verizon reported it received in the first half of 2015. *See* "Verizon's Transparency Report for the First Half of 2015," *available at* http://transparency.verizon.com/us-report?/us-data.

19. These statistics come from dividing the number of all location information demands by the total number of law enforcement

user data sent to AT&T thus far in 2015 are for location information, up from 13% in 2013.[20]

The majority of these demands for detailed location information are made without a warrant. Verizon has reported that two-thirds of all law enforcement requests for location information, not including tower dumps, were made via a court order, like the order issued under the Stored Communications Act the government obtained here.[21] Such orders only require the government

---

requests as reported by Verizon to Senator Edward Markey and in its transparency reports. In 2012, of the 270,000 demands made to Verizon, approximately 30,000, or 11%, were for location data. *See* Oct. 3, 2013 Letter from William Petersen, Verizon Wireless General Counsel to U.S. Senator Edward Markey (D-Mass.) at p. 2-3, *available at* http://publicpolicy.verizon.com/assets/docs/Markey_Letter_Oct_3_2013.pdf. In the first six months of 2015, of the 149,810 law enforcement requests for information Verizon received, 25,210 or 16%, were for location information. *See* Verizon Transparency Report for the First Half of 2015, *available at* http://transparency.verizon.com/us-report.

20. AT&T reported that it received 277,132 demands for customer information in criminal investigations in 2013. Of those requests, 37,839, or 13%, were for location information. *See* 2014 AT&T Transparency Report at p. 3-4, *available at* http://about.att.com/content/dam/csr/Transparency%20Reports/Transparency/ATT_Transparency%20Report_Jan%202014.pdf. In the first six months of 2015, AT&T reported it received 133,903 demands for customer information in the context of criminal investigations. Of those requests, 37,973, or 28%, were for location information. *See* AT&T Transparency Report for the First Half of 2015, *available at* http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html.

21. *See* Verizon Transparency Report for the First Half of 2015, *available at* http://transparency.verizon.com/us-report ("In the

demonstrate reasonable grounds to believe that the data is "relevant and material" to an ongoing criminal investigation, rather than probable cause that evidence of criminal activity will be found, the standard required to obtain a warrant. *See* 18 U.S.C. § 2703(d); *Illinois v. Gates*, 462 U.S. 213, 239 (1983) ("An affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause").

However, as this Court has repeatedly noted, "the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'" *Riley*, 134 S.Ct. at 2493 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)). Where, as here, the data available to law enforcement can reveal personal and private information, not just about a person's whereabouts over time, "but also [about] the people and groups they choose to affiliate with and when they actually do so," *State v. Earls*, 70 A.3d 630, 642 (N.J. 2013), a warrant should be required.

---

first half of this year, we received approximately 21,800 demands for location data: as in the past, about two-thirds of those were through orders and one-third were through warrants."). Although Verizon has not broken down what percentage of requests for "cell tower dumps" are done with a warrant, it does make clear that it does not always demand a warrant before turning this information over to law enforcement. *See id.* ("In addition, we received approximately 3,410 warrants or *court orders* for 'cell tower dumps' in the first half of this year. In such instances, the warrant or *court order* compelled us to identify the phone numbers of all phones that connected to a specific cell tower during a given period of time.") (emphasis added).

D. *Certiorari* Is Necessary to Resolve the Judicial Split on Whether a Warrant Is Required to Obtain CSLI, Particularly as Americans Expect These Records to Remain Private.

As cell phones and smartphones permeate society, many courts and legislatures have responded to the public's recognition that location information stored on and generated by mobile phones deserves "the most scrupulous protection from government invasion." *Oliver v. United States*, 466 U.S. 170, 178 (1984) (citation omitted). That means, contrary to the Eleventh Circuit's conclusion, it is reasonable to expect that cell site location information will be kept private.

A "Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo*, 533 U.S. at 33 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). Societal expectations, in turn, must have "a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143-44, n. 12 (1978)) (quotations omitted). 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." *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759 (2010).

Recent studies show Americans expect privacy when it comes to location information. Within the last

year, 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.[22] In 2012, the Pew Research Center found that cell phone owners take a number of steps to protect access to their personal information and mobile data, and more than half of phone owners with mobile apps have uninstalled or decided to not install an app due to concerns about the privacy in their personal information.[23] In addition, more than 30% of smart phone 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 for other uses—and 32% cleared their browsing or search history.[24] The numbers are higher for teenagers, with Pew reporting 46% of teenagers turned location services off.[25] A 2013 survey conducted on behalf of the Internet company TRUSTe found 69% of American

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

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

24. *Id.*

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

smart phone users did not like the idea of being tracked.[26] And a 2009 Carnegie Mellon survey of perceptions about location-sharing technologies showed that participants believed the risks of location-sharing technologies outweighed the benefits and were "extremely concerned" about controlling access to their location information.[27]

The idea that it is objectively reasonable to find historical cell site location information private and to require the government use a probable cause search warrant to obtain this sensitive data has found wide support in both federal and state courts.[28] Similarly, state

---

26. 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/.

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

28. For cases decided in the last two years finding a warrant is required for the government to obtain historical cell site records, *see, e.g., Graham*, 2015 WL 4637931, at *8; *In re Application for Tel. Info.*, 2015 WL 4594558, at *23; *United States v. Cooper*, 2015 WL 881578, *8 (N.D. Cal. Mar. 2, 2015) (unpublished); *Augustine*, 4 N.E.3d at 866, *Earls*, 70 A.3d at 644. For cases decided in the last two years adopting a warrant requirement for real time cell phone tracking, *see, e.g., United States v. White*, 62 F.Supp.3d 614, 622-23 (E.D. Mich. 2014); *United States v. Powell*, 943 F.Supp.2d 759, 776-79 (E.D. Mich. 2013); *Tracey v. State*, 152 So.3d 504, 526 (Fla. 2014); *Commonwealth v. Rushing*, 71 A.3d 939, 961-64 (Pa. Sup. Ct. 2013), *overruled on other grounds* 99 A.3d 416 (2014).

legislatures have also acted, with eleven states passing laws requiring police use a warrant to obtain various forms of cell phone location information.[29]

This support is not uniform, however, and some courts—like the Eleventh Circuit here—have reached the opposite conclusion. *See, e.g. Davis*, 785 F.3d at 511; *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 615. But the fact that reasonable jurists can disagree undermines the Eleventh Circuit's conclusion that an expectation of privacy in cell site location records "is not justifiable or reasonable." *Davis*, 785 F.3d at 511. Nor can the Eleventh Circuit dismiss the existence of an expectation of privacy when an increasing number of Americans have been promised the protections of a search warrant by case law or statute.

Given the prevalence of cell phones and smart phones, and the increasing number of law enforcement requests for this sensitive information, this case thus presents a question of compelling national importance. The number of Americans promised that CSLI remains private and accessible to law enforcement only with the protections of

29. Maine, Minnesota, Montana, Tennessee and Utah have passed laws requiring police use a warrant to obtain historical cell site location information. *See* 16 Maine Rev. Stat. Ann. § 648; Minn. Stat. Ann. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); Tenn. Code Ann. § 39-13-610(b); Utah Code Ann. § 77-23c-102(1)(a). Six other states—Illinois, Indiana, Maryland, Virginia, Washington and Wisconsin—have passed laws requiring police obtain a search warrant to track a cell phone in real time. *See*, 725 Ill. Comp. Stat. 168/10; Ind. Code § 35-33-5-12; Md. Code, Criminal Procedure 1-203.1(b)(1); Va. Code Ann. 19.2-56.2(b); Wash. Rev. Code 9.73.260; Wis. Stat. Ann. § 968.373(2).

a search warrant is increasing. Yet, this legal protection is not uniform, and the federal courts in particular have issued conflicting opinions on the topic, leaving the public and law enforcement in limbo.

This Court should therefore grant *certiorari* 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.

CONCLUSION

"With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities." *Arizona v. Evans*, 514 U.S. 1, 17-18 (1995) (O'Connor, J., concurring). Given the government's newfound ability to track people for extended periods of time through cell site location information, the corresponding constitutional responsibility is to insist police use a probable cause search warrant to obtain this sensitive information.

This Court should grant Mr. Davis' petition for a writ of *certiorari*.

Dated: August 31, 2015 Respectfully submitted,

Jeffrey T. Green
Co-Chair, Amicus Committee
National Association of
Criminal Defense Lawyers
1660 L Street, NW
Washington, DC 20036
(202) 872-8600

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

Hanni M. Fakhoury
Counsel of Record
Jennifer Lynch
Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
hanni@eff.org

Counsel for Amici Curiae