No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES

Respondent.

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

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, BRENNAN CENTER FOR JUSTICE, THE CONSTITUTION PROJECT, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AND NATIONAL ASSOCIATION OF FEDERAL DEFENDERS IN SUPPORT OF PETITIONER

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

Counsel for Amici Curiae

(Additional Counsel listed inside cover)

274756

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

Faiza Patel
Michael W. Price
Rachel Levinson-Waldman
Brennan Center for Justice
at NYU School of Law
161 Avenue of the Americas,
12th Floor
New York, NY 10013

Counsel for Brennan Center for Justice at NYU School of Law

Jake Laperruque
The Constitution Project
1200 18th Street NW,
Suite 1000
Washington, DC 20036

Counsel for The Constitution Project

David Oscar Markus
Co-Chair, Amicus Committee
National Association
of Criminal Defense
Lawyers
40 NW Third Street, PH1
Miami, FL 33128

Counsel for National Association of Criminal Defense Lawyers

Meghan Skelton
Donna Coltharp
Sarah Gannett
Dan Kaplan
Co-Chairs, NAFD Amicus Committee
National Association of
Federal Defenders
850 West Adams Street,
Suite 201
Phoenix, AZ 85007

Counsel for National Association of Federal Defenders

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

CASES

Cited Authorities

Page

Page

STATUTES

Cited Authorities

Page

CONSTITUTIONAL PROVISIONS

LEGISLATIVE AUTHORITIES

OTHER AUTHORITIES

Cited Authorities

Page

Page

Page

STATEMENT OF INTEREST[1]

Amici are organizations committed to ensuring that constitutional rights are protected as technology advances and include the Electronic Frontier Foundation, Brennan Center for Justice, the Constitution Project, National Association of Criminal Defense Lawyers, and National Association of Federal Defenders. All of these organizations have appeared previously as *amici* before this Court. Their individual organizational statements are contained in the Appendix following this brief.

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 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. The parties' letters consenting to the filing of all *amicus* briefs have been filed with the Clerk's office. Pursuant to Supreme Court Rule 37.6, *amici* state that 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. This brief does not purport to represent the position of NYU School of Law.

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—to be usable at all—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, they "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*, 565 U.S. 400, 415 (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. Yet law enforcement obtains this type of information without a warrant, tens of thousands of times a year.

This case requires the Court to address whether the Fourth Amendment prohibits the warrantless seizure and search of CSLI.[2] The Sixth Circuit below relied on this Court's opinion in *Smith v. Maryland*, 442 U.S. 735 (1979), to hold Americans lack a reasonable expectation

2. The issues in this case are highly similar to *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016), which remains pending on a petition for certiorari in this Court. *See* No. 16-6308.

of privacy in CSLI because it is a business record held by third-party service providers. *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016).

But *Smith* cannot govern here. The now-routine use of CSLI to reconstruct individuals' movements over extended periods of time was "nearly inconceivable just a few decades ago," *Riley*, 134 S. Ct. at 2484. Whatever wisdom the so-called third-party doctrine had in 1979 when *Smith* was decided, it is entirely "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*, 565 U.S. at 417 (Sotomayor, J. concurring). The Court should instead hold that CSLI is subject to the full protection of the Fourth Amendment.

ARGUMENT[3]

Americans carry their cell phones with them everywhere and, as they do, they automatically generate granular and detailed information about where they have been, and when. The amount of sensitive location data generated by cell phones has increased dramatically in recent years, matched only by the increase in warrantless law enforcement demands for it. But if the Fourth Amendment is to have any force in the digital age, then it must keep up with how Americans use cell phone technology. Using CSLI to determine individuals' movements is as revealing as the GPS tracking this Court found problematic in *Jones*, if not more so. And because

3. All websites cited in this brief were last visited on August 8, 2017.

CSLI is becoming more precise over time, it can rival GPS tracking in geographical accuracy.

Applying the third-party doctrine to CSLI is inconsistent with the original reasoning underlying this Court's third-party doctrine cases. These cases stand for the proposition that individuals lose their expectation of privacy in certain records they "voluntarily" convey to third parties. But CSLI is purely a byproduct of owning and carrying an operational phone—it is automatically created whenever the phone tries to send and receive information, generally without forethought or conscious action by the owner. And cell phones are so essential to modern life that it is practically impossible to avoid creating CSLI in the first place. As a result, individuals do not "voluntarily" convey this information to cellular providers in any normal sense of the word. Instead, Americans overwhelmingly consider location privacy important and many take steps to limit sharing of their location.

Finally, CSLI implicates the same kind of expressive and associational activities that the Framers sought to safeguard in the Fourth Amendment. They specified that "papers" are protected against unreasonable searches and seizures to ensure that the warrant requirement applied in full force when these rights were at stake—as in this case. This Court should recognize the First Amendment functions that cell phones play in the digital age and grant CSLI the Fourth Amendment's full protection.

I. There Has Been a Dramatic Increase in Location Data Generated by Cell Phones, Collected by Third Parties, and Routinely Obtained by Law Enforcement Without a Warrant.

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

Owning a cell phone is not a luxury; at least 95% of all American adults have a cell phone, and most carry their phone with them everywhere they go.[4] As the Court explained 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.

The first commercial cell phone service was offered in the United States in 1983[5]—four years after this Court's 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 396 million—72 million more accounts than people at the end of 2016.[6]

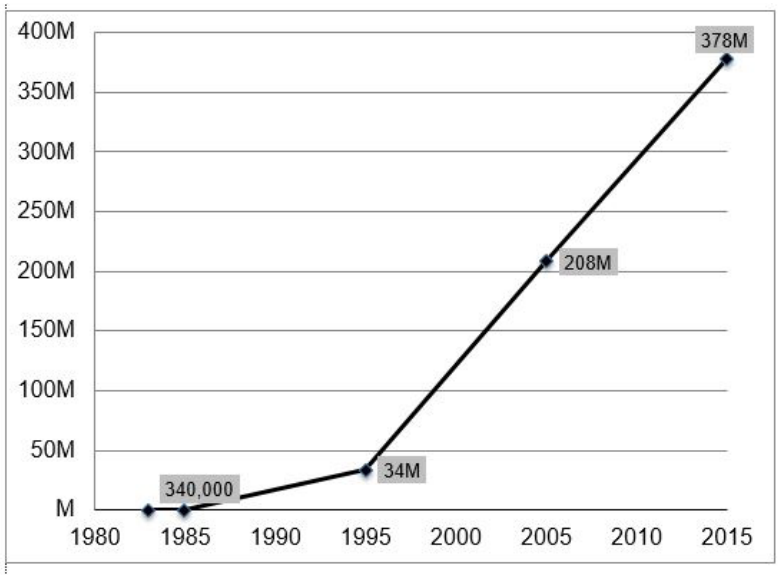
---

4. *See Mobile Fact Sheet*, Pew Research Center (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile; *2013 Mobile Consumer Habits Study* 2–3, Harris Interactive (June 2013), 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.

6. CTIA—The Wireless Association, *Annual Year-End 2016 Top-Line Survey Results* 3 (May 2017) ("CTIA 2016 Survey"),

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



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

---

https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf (396 million "wireless subscriber connections"); *see* U.S. Census Bureau, *U.S. and World Population Clock*, http://www.census.gov/popclock (estimated U.S. population 324 million on December 31, 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—The Wireless Association, *Annual Year-End 2015 Top-Line Survey Results* 3 (May 2016) ("CTIA 2015 Survey"), *available at* http://bit.ly/2h38cS4.

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] There are at least 300,000 cell sites operating in the United States,[10] and these sites include many more antennae constantly communicating with all phones in range.[11]

---

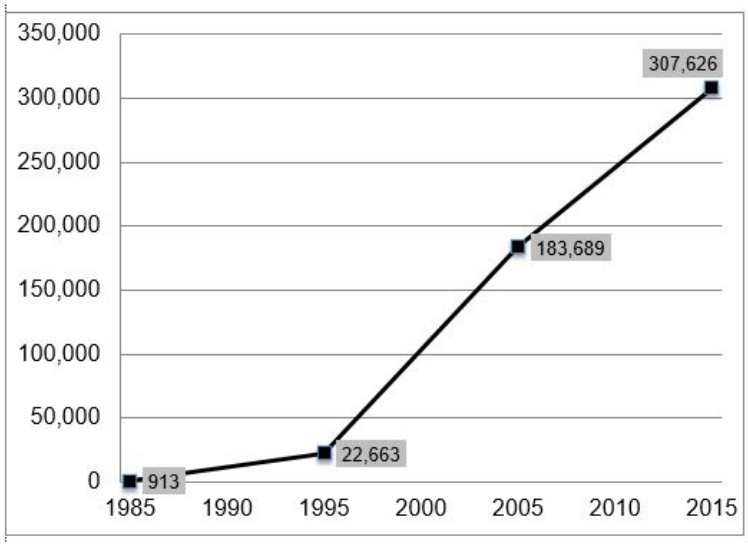
8. *See* Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary, 113th Cong. 50, at 6, 9 (2013) (written testimony of Professor Matt Blaze, University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

9. 2013 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 2016 Survey at 4 (308,334 cell sites in 2016).

11. A different estimate reports 645,891 towers and 1,892,359 antennae—including those used for cellular and other communications services—as of July 9, 2017. AntennaSearch.com, http://antennasearch.com.

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 in popularity. Now more than 77% 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 10.

13. *Mobile Fact Sheet*, Pew Research Center; CTIA 2016 Survey at 2 (262 million smartphones in use in 2016).

14. 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-

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—3,500% between 2010 and 2016 alone[15]—and service providers have installed more towers to handle that increase.[16]

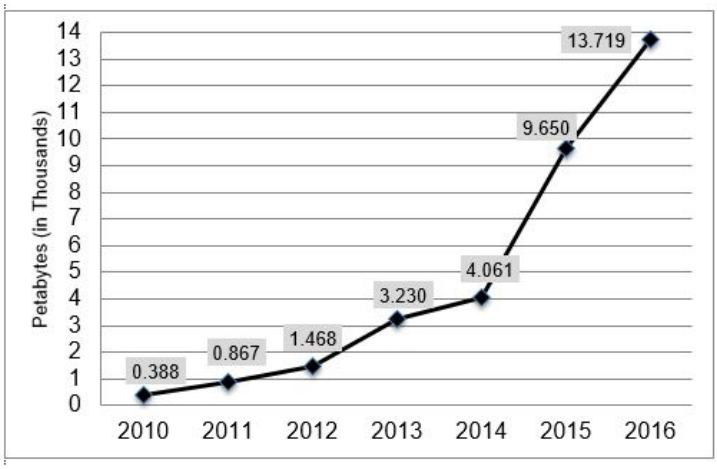
---

and-their-smartphones (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%)).

15. CTIA 2016 Survey at 3 (388 billion megabytes in 2010, 13,719 billion megabytes in 2016).

16. 2013 Blaze Testimony at 11.

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



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.

---

17. CTIA 2016 Survey at 4. 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.

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, sending and receiving 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 that 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 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 traveled. Cell providers store this data for up to five years[20] and can also track CSLI in near real-time.[21]

---

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).

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).

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 (4th Cir. 2015) *vacated by* 824 F.3d 421 (4th Cir. 2016) (en banc). 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. With newer cell technology, providers can determine not just the location of the cell site the phone connects to, but, by "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

22. 2013 Blaze Testimony at 10.

23. *Id*. at 12.

24. *Id*.

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. In these areas, the higher concentration of towers and antennae allow phones' locations to be pinpointed with even greater accuracy.[27]

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 70,528 requests for CSLI in 2016 and 76,340 requests in 2015.[28] Verizon received 53,532

---

25. *Id.* at 11.

26. *Id.* at 12.

27. *Id.* at 10-12.

28. *See* AT&T, *AT&T Transparency Report* 4, 8 (Feb. 2017), http://about.att.com/content/dam/csr/Transparency%20Reports/Feb-2017-Transparency-Report.pdf; AT&T, *AT&T Transparency Report* 4 (Jan. 2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_Jan%202016.pdf (disclosing number of 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).

requests in 2016 and 50,066 requests in 2015.[29] T-Mobile, the parent company of MetroPCS and the service provider in this case, *Carpenter*, 819 F.3d at 885, does not report requests for CSLI specifically, but the company received far more requests for customer data as a whole than its much larger rivals.[30]

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 this case, officers relied on three requests to access information about 16 different phones. *Carpenter*, 819 F.3d at 884. The quantity of data requested for each phone may vary, although a

---

29. *See* Verizon, *Verizon's Transparency Report for the Second Half of 2016: U.S. Report* (2017), http://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2017/01/Transparency-Report-US-2H-2016.pdf; Verizon, *Verizon's Transparency Report for the First Half of 2016: U.S. Report* (2016), https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report-US-1H-2016.pdf; Verizon, *Verizon's Transparency Report for the Second Half of 2015* (2016), https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report-US-2H-2015.pdf; Verizon, *Verizon's Transparency Report for the First Half of 2015* (2015), https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/01/Verizon-Transparency-Report-2015-first-half.pdf (numbers include "location information" and cell tower dumps).

30. 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; T-Mobile, *T-Mobile Transparency Report for 2015*, *available at* https://newsroom.t-mobile.com/content/1020/files/2015TransparencyReport.pdf.

single request often produces CSLI that covers very long periods. Here, the FBI obtained three to four months of data, 819 F.3d at 895 (Stranch, J., concurring), while in *Graham*, agents were able to obtain 221 days of location information for Mr. Graham and his co-defendant with a single request. 796 F.3d at 341 (panel opinion).

The majority of these demands for CSLI are warrantless. In 2016, Verizon reported that up to three-quarters of all law enforcement requests for historical and real-time location information were made via a court order rather than warrant,[31] like the orders issued under 18 U.S.C. § 2703(d) that the government obtained in both this case 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*, 565 U.S. at 415 (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 Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005).

---

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

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*, 565 U.S. at 430 (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*.[32]

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, unlike GPS monitoring of a vehicle, examination of historical CSLI over an extended period as in this case cannot be confined to public spaces and "will invariably enter constitutionally protected areas, such as private residences." *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1023; *Tracey*, 152 So. 3d at 524 (real time "cell phone tracking can easily invade the right to privacy in one's home or other private areas, a matter that the government cannot always anticipate and one which, when it occurs,

32. According to one estimate, covert car pursuit can cost $275 per hour while location tracking via a cell phone can cost as little as $0.04 per hour, meaning that CSLI has increased government's capacity to track individuals by a factor of thousands. *See* Kevin Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. Online 335 (2014), http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

is clearly a Fourth Amendment violation."). And, in fact, using records about a defendant in *Graham*, the ACLU was able to infer details about his patterns of movement and presence in private spaces, including when he and his pregnant wife visited her obstetrician, when he traveled to or from his home, and nights spent away from home.[33]

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* 565 U.S. at 430 (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 413 (Sotomayor, J., concurring). Here, the government obtained 88 days and 127 days worth of location information from each defendant respectively. In other cases, the government has sought similarly extended periods of records, up to seven months of location information worth in a single request. *Davis*, 785 F.3d at 501 (67 days); *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) (113 days); *United States v. Jones*, 908 F. Supp. 2d 203, 206 (D.D.C. 2012) (180 days); *Graham*, 796 F.3d at 349 (221 days). 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

33. *See* Bennett Stein, *Fighting a Striking Case of Warrantless Cell Phone Tracking*, ACLU (July 1, 2013), https://www.aclu.org/blog/fighting-striking-case-warrantless-cell-phone-tracking (noting records were analyzed with Mr. Graham's "assistance and permission").

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, 463 (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 *Jones*, tracking a car's location for 28 days "would have [traditionally] required a large team of agents, multiple vehicles, and perhaps aerial assistance." 565 U.S. at 429 (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 that 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*, 565 U.S. at 429 (Alito, J., concurring in the judgment).

III. The Third-Party Doctrine Is "Ill-Suited to the Digital Age" and Should Not Apply to CSLI.

The majority opinion in *Carpenter* relied on this Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979) (citing *United States v. Miller*, 425 U.S. 435, 442 (1976)), to hold that the Fourth Amendment does not protect CSLI. *Smith* is the principal basis for the so-called third-party doctrine, which the government argues denies Fourth Amendment protection for some information that is "voluntarily" conveyed to "third parties." But as Justice Sotomayor suggested in *United States v. Jones*, the third-party doctrine is "ill suited to the digital age" and should not now be extended to modern communications data like CSLI. 565 U.S. at 417 (Sotomayor, J., concurring).

First, disclosing CSLI to a service provider is not "voluntary" in any realistic sense of the word. Cell phones create CSLI constantly and automatically, even when they are not in active use. Moreover, they have become essential to daily life, and are crucial vehicles for First Amendment activity. Requiring Americans to forgo their phones in exchange for privacy would therefore present an untenable choice that is inconsistent with the history and purpose of the Fourth Amendment.

Second, the third-party doctrine is at odds with the way technology works and how people communicate today. Relying on *Smith*, some courts have mistakenly viewed information as either completely secret or presumptively public, failing to account for more nuanced understandings of privacy.

Finally, the third-party doctrine rests on outdated expectations about the "assumption of risk" involved in

making a phone call that fail to account for the modern First and Fourth Amendment implications of data like CSLI. Communications data should command heightened constitutional protections, and at minimum, a warrant requirement.

A. Cell Phone Users Do Not "Voluntarily Convey" CSLI to Service Providers.

In *Katz*, the Court pointed out that individuals could exercise their right to privacy in a public phone booth by remembering to close the phone booth door, thereby taking an affirmative step to exclude the "uninvited ear." *Katz v. United States*, 389 U.S. 347, 352 (1967). But for cell phone users, there is no door, no possible way to protect the privacy of personal data like CSLI. Exposing one's location to service providers through CSLI is an inescapable part of having a cell phone. There is no practical alternative, no option to mask the metadata,[34] no way to close the proverbial phone booth door. *See Katz*, 389 U.S at 352.

i. The Vast Majority of CSLI Is Generated Automatically.

It is a Fourth Amendment fiction that individuals "voluntarily" convey CSLI as one would dial a phone number. Users do not intentionally create CSLI and

34. Many smartphones include a location privacy setting that, when enabled, prevents applications from accessing the phone's location. However, this setting has no impact on a carrier's ability to learn the cell sector in use, thus giving phone users a false sense of privacy. *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1025.

have no real choice in the matter. In fact, it is "unlikely that cell phone customers are [even] aware that their cell phone providers collect and store historical location information." *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 (3d Cir. 2010); *see also United States v. Stimler,* Nos. 15-4053, 15-4094, 15-4095, 2017 WL 3080866, at *5 (3d Cir. July 7, 2017) (users do not voluntarily disclose CSLI to service providers); *Augustine*, 4 N.E.3d at 862 (same).

Rather, as described above, phones generate CSLI whenever they are on and searching for a signal—frequently, automatically, and regardless of whether the device is actively in use. CSLI includes data generated when users make calls, but that is a drop in the bucket compared to 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, the amount of data produced by such "passive" activities dwarfs the number of records from actually making phone calls, and is 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 unwitting 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.

ii. There Is No Reasonable Alternative to Conveying CSLI to Third-Party Service Providers.

The only way to avoid producing a comprehensive record of one's movements and associations based on CSLI is to stop carrying a cell phone, as some courts have suggested. *See, e.g., Carpenter,* 819 F.3d at 888; *Graham*, 824 F.3d at 427-28. But if a cell phone can be considered a "feature of human anatomy," then owning and carrying one is hardly a choice at all. *Riley*, 134 S. Ct. at 2484. Given that nearly all American adults own a cell phone, the position that cell phone users volunteer their location information simply by choosing to activate and use their phones and to carry the devices is untenable and unrealistic. *See State v. Earls*, 70 A.3d 630, 641 (N.J. 2013).

Furthermore, as this Court has repeatedly recognized, cell phones have become essential to the exercise of First Amendment freedoms. Indeed, they are "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010); *Riley*, 134 S. Ct. at 2484; *see also United States v. Cooper*, No. 13–cr–00693–SI–1, 2015 WL 881578, at *8 (N.D. Cal. March 2, 2015) (cell phones are "ubiquitous, and for many, an indispensable gizmo to navigate the social, economic, cultural and professional realms of modern society."). Privacy cannot be the price of exercising those First Amendment freedoms.

B. The Third-Party Doctrine Is Incompatible with Modern Communications, and Americans Reasonably Expect Location Data to Remain Private.

The third-party doctrine is an exceedingly blunt instrument. In its strongest formulation, it divides the world in half: data is either completely secret or it is not private at all. But in practice, the privacy of communications metadata like CSLI is not an all-or-nothing endeavor. Some people may affirmatively choose to disclose their location information publicly, as when "geotagging" a Tweet.[35] On the other hand, people may restrict affirmative sharing of their location information to a more limited audience, like family or close friends.[36] And at other times, users may not consciously opt to share their location with anyone at all. But even the decision to "turn off" location sharing has no effect on the ability of service providers to know where a subscriber's phone is, assuming it is working and connected to their network. *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1025. If the third-party doctrine were to apply in this context, then the whereabouts of every cell phone user in America would never be private for Fourth Amendment purposes, no matter which other human beings—if any—they actually shared that information with.

---

35. *See* Twitter, *FAQs About Adding Location to Your Tweets*, https://support.twitter.com/articles/78525.

36. *See* Apple, *Share Your Location With Your Family*, https://support.apple.com/en-us/HT201087 (describing how Apple users can share their iPhone location with family members, with select family members, or no one at all).

In fact, recent studies show that Americans generally expect their location information to remain private, even though they may at times share it with others. 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.[37] In 2012, another Pew 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.[38] Additionally, more than 30% of smartphone owners polled took affirmative steps to safeguard their privacy and 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).[39] The numbers are higher for teenagers, with nearly half of all teenagers turning location services off.[40] A 2013 survey conducted on behalf of Internet company TRUSTe found

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

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

39. *Id.*

40. 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/.

69% of American smartphone users were concerned about being tracked.[41]

Correspondingly, the Court should decline to adopt a blanket rule that CSLI lacks Fourth Amendment protection simply because it is shared with a third party. Indeed, the Court's decisions in *Smith* and *Miller* should not be read to endorse open-ended application of the third party doctrine in this way. The Court has repeatedly found that the Fourth Amendment protects some types of personal information, even if it is exposed to a third-party. *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); *see also 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 are entitled to constitutional protection even though they provide "implied or express permission" for third parties to access their rooms). Communications data, like CSLI, should receive at least as much constitutional protection, even if individuals "voluntarily" convey it through third-party service providers.

In this light, applying the third-party doctrine to CSLI would defy Americans' expectations about privacy and disregard the decisions they actually make about what information to share. *Cf. Oliver v. United States*,

41. 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.

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"). It would also allow for the warrantless tracking of the historical movements of anyone who carries a cell phone—nearly the entire population of the country.

Fortunately, the Court made clear in *Smith* itself that a "normative inquiry" would be necessary if individuals were not accorded a reasonable expectation of privacy consistent with "well-recognized Fourth Amendment freedoms." 442 U.S. at 740 n.5. In other words, the Fourth Amendment must protect CSLI to put limits on the "power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34.

C. Cell Phone Location Information Implicates First Amendment Interests that Require Fourth Amendment Protection.

Cell phone location information implicates the kind of expressive and associational activities that the Fourth Amendment was designed to protect. By giving "papers" equal billing with "persons," "houses," and "effects," the Framers indicated that courts have a special obligation to safeguard First Amendment information from unreasonable searches and seizures. *See* U.S. Const. amend. IV; *Marcus v. Search Warrants of Prop. at 104 E. Tenth St.*, 367 U.S. 717, 729 (1961) ("The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."); *Stanford*

v. Texas, 379 U.S. 476, 482 (1965) (describing the history of the Fourth Amendment as "largely a history of conflict between the Crown and the press").

Accordingly, courts should apply the Fourth Amendment's warrant requirement with "scrupulous exactitude" when significant First Amendment rights are at stake. *Stanford*, 379 U.S. at 485; *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *see also New York. v. P. J. Video*, 475 U.S. 868, 873-75 (1986) (films); *Maryland v. Macon*, 472 U.S. 463, 468 (1985) (magazines); *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (letters); *Walter v. United States*, 447 U.S. 649, 655 (1980) (books). A search or seizure that endangers First Amendment interests must, at the least, be made pursuant to a warrant supported by probable cause. *See Zurcher*, 436 U.S. at 565; *Roaden v. Kentucky*, 413 U.S. 496, 504 (1973) (requiring a warrant to seize an allegedly obscene film because "[t]he setting of the bookstore or the commercial theater ... invokes such Fourth Amendment warrant requirements").

In *Riley*, the Court reinforced this approach by requiring a warrant for cell phone searches incident to arrest because "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated" by most physical searches. 134 S. Ct. at 2488-89. Significantly, the unanimous Court was alarmed that a warrantless search would yield not only text messages and emails, but also "*[h]istoric location information*" that "can reconstruct someone's movements down to the minute, not only around town but also within a particular building." 134 S. Ct. at 2490 (emphasis added). Citing Justice Sotomayor's concurrence in *Jones*, the Court determined that such information is qualitatively different

from physical records (like those in *Smith*, perhaps) because such a "comprehensive record of a person's public movements . . . reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* (citing *Jones*, 565 U.S. at 415).

The common denominator in these decisions is that the data implicates the protected expressive and associational information the Framers sought to shield from warrantless government interference. Of course, the phone records in *Smith* involved private communications as well. 442 U.S. at 742. But comparing phone records in 1979 to communications metadata in 2017 is like "saying a ride on horseback is materially indistinguishable from a flight to the moon." *See Riley*, 134 S. Ct. at 2488; *see also United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (distinguishing the search of a laptop from the search of hand luggage because "technology matters").

Not only is the creation of CSLI unavoidable, but it is also simple to infer otherwise private expressive and associational activities from it in ways that were highly unlikely in *Smith*. This recognition again undercuts the "voluntariness" rationale at the heart of the third-party doctrine. Phone users in 1979 may have "assumed the risk" that the numbers they dial could be divulged to police, *Smith,* 442 U.S. at 745, but they did not assume they would be disclosing their religion, political affiliation, or sexual preferences—and neither did the Justices.

Even in limited quantities, these staccato signals can be a telltale sign of social, political, and religious activities. As in the GPS-tracking context, CSLI can reveal other activities of "indisputably private nature,"

like a visit to the "psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 909 N.E.2d 1195, 1999 (N.Y. 2009)).

The third-party doctrine advanced in *Smith* may have been appropriate for phone calls in 1979, but it is a poor match for the digital age. Communications data, like CSLI, has such significant First Amendment implications that it demands Fourth Amendment protection. *See Roaden*, 413 U.S. at 504 (the Court should examine Fourth Amendment reasonableness "in the light of the values of freedom of expression"); *Stanford*, 379 U.S. at 485; *Zurcher*, 436 U.S. at 564; *see also* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. Nat'l Security L. & Pol'y, 270-71 (2015). CSLI implicates the same kind of expressive and associational activities that the Framers sought to protect by including "papers" in the text of the Fourth Amendment, and this Court should guard it accordingly. *See Riley*, 134 S. Ct. at 2491 (Fourth Amendment requires "clear guidance to law enforcement through categorical rules").

CONCLUSION

For the reasons stated above, this Court should hold that sensitive records like cell site location information are protected by the Fourth Amendment's warrant requirement.

Dated: August 14, 2017

Respectfully submitted,

Faiza Patel
Michael W. Price
Rachel Levinson-Waldman
Brennan Center for Justice
at NYU School of Law
161 Avenue of the Americas,
12th Floor
New York, NY 10013

Counsel for Brennan Center for Justice at NYU School of Law

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

Counsel for Amici Curiae

Jake Laperruque
The Constitution Project
1200 18th Street NW,
Suite 1000
Washington, DC 20036

Counsel for The Constitution Project

David Oscar Markus
Co-Chair, Amicus Committee
National Association of Criminal Defense Lawyers
40 NW Third Street, PH1
Miami, FL 33128

Counsel for National Association of Criminal Defense Lawyers

Meghan Skelton
Donna Coltharp
Sarah Gannett
Dan Kaplan
Co-Chairs, NAFD Amicus Committee
National Association of Federal Defenders
850 West Adams Street,
Suite 201
Phoenix, AZ 85007

Counsel for National Association of Federal Defenders

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*, 565 U.S. 400 (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*, 565 U.S. 400 (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 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 Federal Defenders ("NAFD"), formed in 1995, is a nationwide, nonprofit, volunteer organization whose membership is comprised of attorneys who work for federal public and community defender organizations authorized under the Criminal Justice Act. Each year, federal defenders represent tens of thousands of individuals in federal court. *Amicus* NAFD therefore has both particular expertise and interest in the subject matter of this litigation.

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, and has a nationwide membership of many thousand direct members, and up to 40,000 members when affiliates are included. NACDL's members include private criminal defense lawyers, public defenders, military

defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. Each year, NACDL files numerous briefs as *amicus curiae* in the United States Supreme Court and other federal and state 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.

This case presents issues of great importance to NACDL and the clients its attorneys represent, including the rights embodied in the Fourth Amendment to be free from constant and pervasive governmental snooping into the most private of our affairs.