No. 16-7314

IN THE

Supreme Court of the United States

ANTONIO RIOS,

Petitioner,

v.

UNITED STATES,

Respondent.

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

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, AND THE CONSTITUTION PROJECT IN SUPPORT OF PETITIONER

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

Attorneys for Amici Curiae

273876

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

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

CASES

Cited Authorities

Cited Authorities

LEGISLATIVE AUTHORITIES

Page

Cited Authorities

Page

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

Cited Authorities

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, the Center for Democracy & Technology, and the Constitution Project. These organizations have appeared previously as amicus curiae before this Court. Their individual organizational statements are contained in the Appendix following this brief.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

This case asks the Court to consider a question left open in *United States v. Jones*: whether real-time tracking of a person's movements "through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy." 565 U.S. 400, 412 (2012). The Sixth Circuit below held that law enforcement did not need a warrant to follow Mr. Rios when it tracked his cell phone location in real time. *United States v. Rios*, 830 F.3d 403, 427-29 (6th Cir. 2016). Because this holding deepens a split of authority with the Florida Supreme Court's ruling in *Tracey v. State,* 152 So. 3d 504, 526 (Fla. 2014), and because such real-time tracking is increasing in frequency and precision, Amici urge the Court to grant certiorari.

---

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

In addition, this case presents equally important—but distinct—factual and legal questions as *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted* 2017 WL 2407484 (June 5, 2017). *Carpenter* involves "historical" location data—generated as a result of a person's cellular usage and already recorded by the provider at the time of a law enforcement request—while this case involves "prospective" location data—generated on an ongoing basis by Mr. Rios' cellular provider *solely* at the direction of law enforcement.[2] *Carpenter* therefore requires the Court to revisit or distinguish its holding in *Smith v. Maryland*, 442 U.S. 735 (1979), that Americans lack a reasonable expectation of privacy in some information held by third-party service providers, whereas this case requires the Court to apply its analyses in *Jones, Kyllo v. United States*, 533 U.S. 27, 34 (2001), and *United States v. Karo*, 468 U.S. 705, 714 (1984), to the precise, inexpensive, and pervasive real-time location tracking technologies available today.

With such real-time tracking, law enforcement can track a person whose identity it may not know, into constitutionally protected spaces, for extended periods of

2. *See* ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 81-85 (2010) (statement of The Honorable Stephen Wm. Smith, United States Magistrate Judge, Southern District of Texas) (explaining that prospective and real-time location data are distinguishable from "historical" location data, which encompasses only location information created, collected, and recorded by the cellular service provider prior to the time the court authorizes a request for that information), *available at* http://judiciary.house.gov/_files/hearings/printers/111th/111-109_57082.pdf.

time, and can pinpoint their location to a high degree of accuracy. The technology can not only convey a person's location within traditionally Fourth Amendment-protected areas like the home, it also can be used to "generate[] a precise, comprehensive record of a person's public movements." *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). It reveals not only a person's daily patterns, but also indisputably private trips, such as to an abortion clinic, AIDS treatment center, strip club, and so on. *People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009).

Therefore, this case once again asks the Court to consider "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34. The Court should grant certiorari to make clear that the Fourth Amendment requires a warrant for all real-time location tracking—whether it is conducted through a GPS device affixed to a person's car, or through location information generated via their cell phone or any other Internet-connected device.

ARGUMENT[3]

Americans carry their cell phones with them everywhere. This generates increasingly granular and detailed information about their location and patterns of movement. The data is not only a byproduct of owning and carrying an operational phone—collected by and stored with third-party service providers—but it may also be generated at law enforcement request by those same service providers, without the user's knowledge.

3. All cited web sites were last visited on June 20, 2017.

The number of cell phones and cell sites is increasing, and real-time tracking technologies are growing more precise. Given the sensitivity of real-time location information, combined with the quantity and extent of law enforcement demands for this data, it is time for this Court to address how the Fourth Amendment applies to real-time cell tracking. The direct split of authority regarding whether a warrant is required to obtain this data only underscores this point.

I. The Court Should Grant Certiorari to Resolve the Direct Conflict Between the Sixth Circuit's Holding in *Rios* and the Florida Supreme Court's Holding in *Tracey v. State*.

In denying Mr. Rios' challenge to the probable cause supporting the warrant for real-time cell phone tracking issued in his case, the Sixth Circuit held that "individuals do not have a reasonable expectation of privacy in the real-time location data that their cellular telephones transmit, making it unnecessary to obtain a warrant to obtain such information." *Rios*, 830 F.3d at 428-29 (relying on *United States v. Skinner,* 690 F.3d 772 (6th Cir. 2012)). This holding is in direct conflict with the Florida Supreme Court's conclusion in *Tracey* that not only do individuals have a "subjective expectation of privacy of location as signaled by one's cell phone—even on public roads," but that expectation is one "that society is now prepared to recognize as objectively reasonable under the *Katz* 'reasonable expectation of privacy' test." 152 So. 3d at 526 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). This Court should grant certiorari to resolve this split in authority and hold that

the Fourth Amendment protects against warrantless real-time cell phone tracking of Americans.

Over the course of the roughly ten years that courts have been considering the Fourth Amendment's application to cell phone location data, there has been intense disagreement over whether a warrant should be required for "real-time" or "prospective" tracking.[4] *See, e.g.*, *Meisler v. Chrzanowski*, No. 3:12-CV-00487-MMD, 2013 WL 5375524, at *20 (D. Nev. Sept. 24, 2013) (noting, after surveying cases, "it goes without saying that the law with respect to whether a warrant based on probable cause . . . is required to obtain disclosure of prospective CSLI is not clearly established."). The Fifth and Sixth Circuits—the only two federal circuit courts that have addressed the issue—have concluded there is no reasonable expectation of privacy in real-time location data broadcast from a phone "voluntarily" used while traveling on public roads. *See Skinner*, 690 F.3d at 777 (citing *United States v. Knotts*, 460 U.S. 276, 281 (1983),

4. The affidavit submitted with the warrant application in Mr. Rios' case describes the property to be seized as "real time precision location information" for a Sprint phone number. Affidavit for Search Warrant, ECF No. 852-1 at 2, *United States v. Rios*, No. 12-cr-00132 (W.D. Mich. Dec. 30, 2013). Many courts refer to "prospective" and "real-time" location data interchangeably. Some have described "real-time" location data as "a subset of prospective location data which includes only information that is both generated after the court's order and is provided to the government in, or close to, 'real time.'" *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 535 n.4 (D. Md. 2011)) ("*Maryland Real-Time Order*") (citations omitted). As a practical matter, these cases all involve *prospective* orders for location information to enable *real-time* tracking, so this brief adopts the terms "prospective location data" and "real-time cell phone tracking."

and noting, "[w]hile the cell site information aided the police in determining Skinner's location [on a public road and at a public rest stop], that same information could have been obtained through visual surveillance"); *United States v. Wallace*, 857 F.3d 685, 690 (5th Cir. 2017) (citing *Skinner* and concluding that the "voluntary disclosure" doctrine adopted by some courts in the context of historical cell site location information (CSLI) applies equally to prospective CSLI and GPS data).

In *Tracey*, the Florida Supreme Court explicitly rejected *Skinner's* analysis, recognizing that real-time cell phone tracking is used not only in situations where law enforcement "could not track [a phone owner] by visual observation" because they do not know the phone owner's whereabouts, but it can also be used to track the phone owner's movements "into clearly protected areas" like the home. 152 So. 3d at 525. Numerous other federal district courts have also recognized this tension.[5] Even the government has conceded that it would infringe upon a person's reasonable expectation of privacy to ask the carrier "to 'ping' the subject's cell phone essentially on a continuous basis while he is in a constitutionally-

5. *See, e.g.*, *Maryland Real-Time Order*, 849 F. Supp. 2d at 540 (cell phone location data is "distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation," which means "that there is no way to know before receipt of location data whether the phone is physically located in a constitutionally-protected place."); *United States v. Powell*, 943 F. Supp. 2d 759, 776 (E.D. Mich. 2013), *aff'd*, 847 F.3d 760 (6th Cir. 2017) ("Under virtually any circumstance, there was no way the DEA could know *in advance* whether or not the location data collected during that period would come from within a protected area.").

protected location." *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 538 (D. Md. 2011) ("*Maryland Real-Time Order*").

Given "the important constitutional issues presented and the conflicting results reached"—including a split between two federal Courts of Appeal and the Florida Supreme Court—the Court should grant certiorari to guide the courts and resolve for the millions of cell-phone-carrying Americans what standard the government must meet before it can turn their phones into real-time tracking devices. *See Heffron v. International Society for Krishna Consciousness*, 452 U.S. 640, 646 (1981).

II. Due to Cell Phones' Technological Capabilities and Widespread Adoption, Prospective Location Data Reveals Private and Increasingly Precise Information About Individuals' Locations and Movements, Counseling in Favor of Certiorari.

A. Service Providers Can Precisely Locate Their Customers, Allowing Law Enforcement to Track Suspects in Real Time.

Because of capabilities built into cell phone networks and handsets in response to federal regulatory requirements, cellular service providers are able to precisely locate cell phones upon law enforcement request. This capability stems from rules adopted in 1996 and implemented by 2001, under which the FCC required cellular service providers to have "the capability to identify the latitude and longitude of a mobile unit making

a 911 call."[6] The precision and accuracy of mandated cell phone location capability is increasing. In January 2015, the FCC adopted new rules to increase law enforcement's ability to locate callers when they are indoors,[7] and to require service providers to develop techniques to determine the altitude of the phone, and thus on which floor of a building it is located.[8]

Although this capability was developed initially to assist in responding to 911 calls, service providers now provide the same location information to law enforcement pursuant to investigative requests. That is, law enforcement can ask a provider to generate new, precise, prospective location data by acquiring information from the target's phone. This can be done "on demand or at periodic intervals."[9] Some providers send periodic location updates via email, while Sprint, Mr. Rios' provider, allows

---

6. Report and Order and Further Notice of Proposed Rulemaking, *In re Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys.*, 11 FCC Rcd. 18676, 18683-84 (1996).

7. *In re Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Fourth Report and Order at 1 (F.C.C. Jan. 29, 2015) ("Wireless E911 Order"), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-9A1.pdf; David Schneider, *New Indoor Navigation Technologies Work Where GPS Can't*, IEEE Spectrum (Nov. 20, 2013) http://spectrum.ieee.org/telecom/wireless/new-indoor-navigation-technologies-work-where-gps-cant.

8. Wireless E911 Order at 3-4.

9. Matt Blaze, *How Law Enforcement Tracks Cellular Phones*, Exhaustive Search (Dec. 13, 2013), http://www.crypto.com/blog/celltapping/.

law enforcement "direct access to users' location data" by logging into an "automated . . . web interface." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc); *see also Maryland Real-Time Order*, 849 F. Supp. 2d at 531 (detailing Sprint's "Precision Locate Service").[10]

The ability to locate and track a phone in real time has no relationship to whether the phone is in use. As long as the phone is on, law enforcement can request that the provider engage location-tracking capabilities; a user cannot disable this functionality.[11] Even modifying location-privacy settings on the phone has no effect on the carrier's ability to determine the phone's precise location in real time. While these settings prevent third-party applications ("apps," like Google Maps) from accessing the phone's location information, they do not impact the carrier's ability to locate the device.

Providers can obtain the location of a cell phone upon law enforcement request in at least two ways, depending on the structure of the carrier's network: (1) by using hardware built into the phone ("handset-

---

10. *See also* Sprint, *Legal Compliance Guidebook* 7 (2008), *available at* https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_concordpd_concordnc.pdf at 568 (guide to requesting precision location from Sprint).

11. *See, e.g. E911 Compliance FAQs*, Verizon Wireless, http://www.verizonwireless.com/support/e911-compliance-faqs/; *How Does E911 Work?*, Sprint, http://www.sprint.com/business/newsletters/articles/e911how_federal01.html.

based" technology); and/or (2) by analyzing the phone's interactions with the network's base stations, or "cell sites" ("network-based" technology).[12] Mr. Rios' service provider, Sprint, uses handset-based technology.[13]

Handset-based technology uses a mobile device's "special hardware that receives signals from a constellation of" GPS satellites.[14] This technology calculates the longitude and latitude of the phone in real time based on the relative strength of radio signals from satellites orbiting the earth.[15] The GPS chip installed in the phone calculates its own location to within 10 meters, or approximately 33 feet.[16] Newer receivers, with enhanced communication-to-

---

12. Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy & Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. on the Judiciary 113th Cong. 6 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) ("2013 Blaze Statement"), *available at* http://judiciary.house.gov/_files/hearings/113th/04252013/Blaze%2004252013.pdf

13. Third Further Notice of Proposed Rulemaking, *In re Wireless E911 Location Accuracy Requirements*, 29 FCC Rcd. 2374, 2414 n.212 (2014) ("Third Notice"), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-13A1.pdf.

14. 2013 Blaze Statement at 7; Wireless E911 Order at 5 n.11.

15. ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 20-21 (2010) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) ("2010 Blaze Statement").

16. 2013 Blaze Statement at 7; Schneider, *supra* note 3; *see also Maryland Real-Time Order*, 849 F. Supp. 2d at 540-

ground-based technologies that correct signal errors, can identify location within three meters or better and have a vertical accuracy of five meters or better 95 percent of the time.[17] GPS accuracy can be enhanced with "dual-frequency receivers" or augmentation systems, which allow for real-time positioning within a few centimeters.[18]

Service providers do not typically maintain GPS coordinate records for phones using their networks, but, upon law enforcement request, they can remotely activate a phone's GPS functionality and then cause the phone to transmit its coordinates back to the provider. *Maryland Real-Time Order*, 849 F. Supp. 2d at 534. They can "ping" phones "unobtrusively, i.e., without disclosing to a telephone user the existence either of the Carrier's signal requesting the telephone to send a current GPS

---

541 (citing U.S. Census Bureau, Median and Average Square Feet of Floor Area in New Single-Family Houses Compared by Location, *available at* http://www.census.gov/const/C25Ann/sftotalmedavgsqft.pdf) ("Given that the average home size in the United States in 2009 was approximately 743 square meters, it is clear that GPS location data . . . would likely place a cellular telephone inside a residence, at least where law enforcement have information regarding the coordinates of the home.").

17. This is sometimes referred to as Assisted GNSS or A-GNSS. Jari Syrjärinne & Lauri Wirola, *Quantifying the Performance of Navigation Systems and Standards for Assisted-GNSS*, InsideGNSS (Sept./Oct. 2008), *available at* http://www.insidegnss.com/node/769; *What is GPS?*, Garmin, http://www8.garmin.com/aboutGPS/; *see also* U.S. Dept. of Defense, *Global Positioning System Standard Positioning Service Performance Standard* v (4th ed. Sept. 2008).

18. GPS Accuracy, "How Accurate is GPS?" GPS.gov, http://www.gps.gov/systems/gps/performance/accuracy/.

reading or that telephone's response." *Id.* at 531 (citing government application).[19]

If a phone is unable to calculate its GPS coordinates, the service provider will "fall back" to a network-based location calculation.[20] Network-based technologies use existing cell site infrastructure, described further below in section II.C, to identify and track location by silently "pinging" the phone and then triangulating its precise location based on which cell sites receive the reply transmissions.[21] Service providers can obtain this cell site location information even when no call is in process. *Maryland Real-Time Order*, 849 F. Supp. 2d at 534.[22] Law enforcement officers can then, as they did in this case, "follow" a suspect in real time "via a computer at the office."[23]

---

19. As described above, this information can be generated upon government request at regular intervals or in near-real time. *See supra* note 4.

20. Third Notice at 2429 n.306.

21. 2013 Blaze Statement at 12; Stephanie Pell & Chris Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 Berkeley Tech. L. J. 117, 128 (2012).

22. Citing The Collection and Use of Location Information for Commercial Purposes: Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection and Subcomm. on Communications, Technology, and the Internet of the H. Comm. on Energy and Commerce, 111th Cong. 3 (2010) (statement of Lori Faith Cranor, Professor of Computer Science and of Engineering & Public Policy, Carnegie Mellon University).

23. Incident Report, ECF No. 852-1 at 13, *United States v. Rios*, No. 12-cr-00132 (W.D. Mich. Dec. 30, 2013).

B. The Significant Increase in the Number of Cell Phones and Cell Sites Allows for Precise Tracking of Any American.

Combined with these technological capabilities, the "element of pervasiveness that characterizes cell phones" has a crucial impact on the Fourth Amendment analysis. *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). Today, owning a cellphone is not a luxury; 95% of Americans have a cell phone, and most carry their phone with them everywhere they go.[24]

The first commercial cell phone service was offered in the United States in 1983[25]—the same year this Court decided *Knotts*. Since that time, the number of mobile device accounts in the United States has grown to an estimated 396 million—71 million more accounts than people.[26]

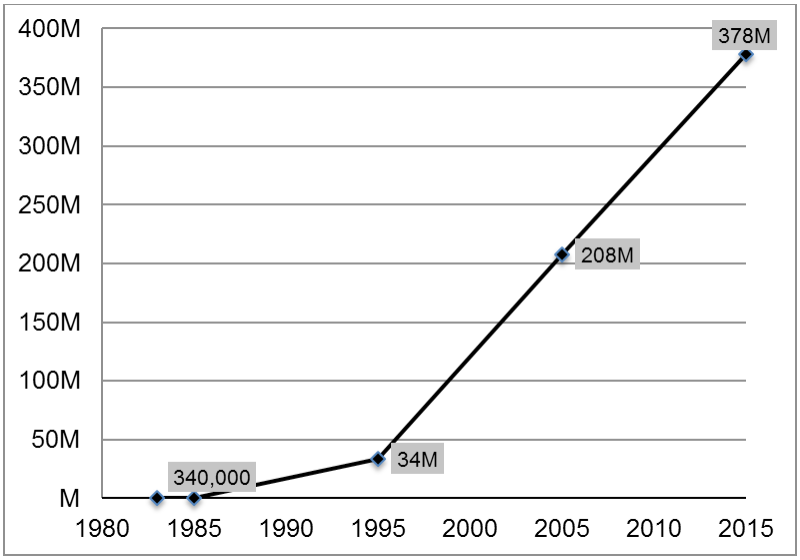
---

24. *See Mobile Fact Sheet*, Pew Research Center (January 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.

25. 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.

26. CTIA—The Wireless Association, *Annual Year-End 2016 Top-Line Survey Results* 3 ("CTIA 2016 Survey"), *available at* 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 325 million on June 8, 2017).

Chart 1: Number of Mobile Device Subscriptions in United States[27]



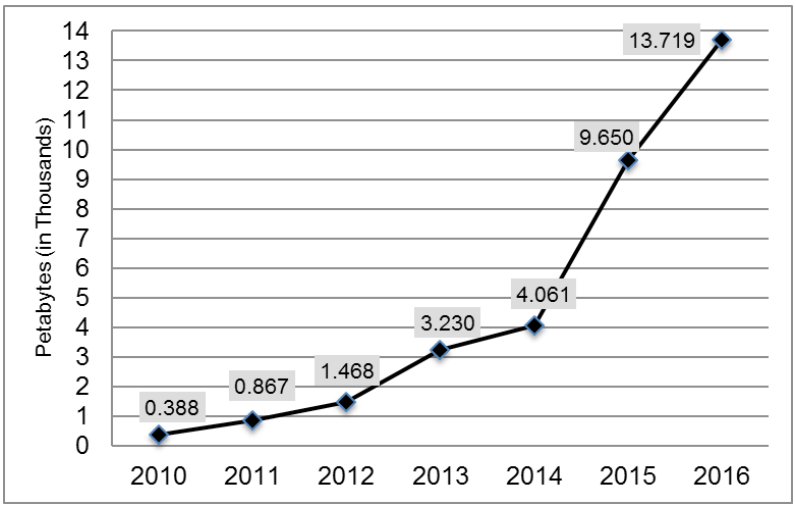
Modern cell phones' increasing sophistication and improved capabilities have dramatically increased the amount of data transmitted by cell phones. Now, more than 77% of Americans own smartphones,[28] which allow users to do everything from take and share photos,

27. Charts were generated using statistics from annual surveys of wireless service providers conducted by CTIA-The Wireless Association, a wireless industry trade association. *See* CTIA—The Wireless Association, *Annual Year-End 2015 Top-Line Survey Results* 3 ("CTIA 2015 Survey"), *available at* https://ctia.org/docs/default-source/default-document-library/ctia_survey_ye_2015_graphics.pdf; CTIA 2016 Survey at 3.

28. *Mobile Fact Sheet*, Pew Research Center; CTIA 2016 Survey at 2.

connect with friends through a variety of video and text-based communication tools, find the fastest route to a new location, research health information, and track finances—and do all of these things at the same time. As more Americans have switched to smartphones, the amount of data transferred over wireless networks has increased significantly—more than 3,500% between 2010 and 2016 alone[29] —and service providers have installed more towers to handle that increase.[30]

Chart 2: Wireless Data Traffic (in Petabytes)[31]



29. CTIA 2016 Survey at 8 (388 billion megabytes in 2010, 13,719 billion megabytes in 2016).

30. 2013 Blaze Statement at 10.

31. CTIA 2015 Survey at 8. One source 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.

C. Law Enforcement Routinely Requests Real-Time Tracking Information, Which Has Become More Precise As Cell Phone Use Has Increased.

When cell phones connect to cell sites, they generate 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 location data 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 cell phone." *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).

Cell phones connect with towers to exchange data on average every seven to nine minutes but can connect as frequently as every seven seconds.[32] These data exchanges create a record of when the user connected to the tower and the location of the tower itself. This reveals where the phone—and by proxy, its owner—is or has been. When law enforcement asks a service provider to conduct prospective tracking using cell tower data, the data generated is precise and frequent enough to allow the police to track a phone in near real time.[33]

---

32. *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).

33. *See Tracey,* 152 So. 3d at 507; *Maryland Real-Time Order*, 849 F. Supp. 2d at 534 ("Due to advances in technology

Law enforcement officers rely on real-time cell phone location tracking to find suspects, even when they do not know who they are looking for. For example, in *Skinner*, authorities could not have found their suspect without electronic tracking because "[a]uthorities did not know the identity of their suspect, the specific make and model of the vehicle he would be driving, or the particular route by which he would be traveling." 690 F.3d at 786 (Donald, J., concurring in part). In this case, detectives were able to arrest Mr. Rios as he drove on a highway due solely to prospective location data generated by Sprint. *United States v. Ruibal,* No. 1:12-CR-132, 2014 WL 357298, at *1-2 (W.D. Mich. Jan. 31, 2014), *aff'd sub nom. Rios*, 830 F.3d 403 (detectives used prospective location data after they "lost visual contact" with Rios' car).

As cell phones saturate the country, law enforcement agencies routinely seek access to real-time location information. The number of these requests is staggering. Mr. Rios' service provider, Sprint, received 30,640 requests for real-time location data in the first half of 2016 and 64,854 requests in 2015.[34] AT&T received 15,971 requests for real-time data in 2016, in addition to 27,162 "exigent" requests, which likely included requests for

---

and the proliferation of cellular infrastructure, cell-site location data can place a particular cellular telephone within a range approaching the accuracy of GPS" (citing 2010 Blaze Statement at 23-27)).

34. Sprint, *Sprint Corporation Transparency Report* 4 (July 2016), *available at* http://goodworks.sprint.com/content/1022/files/Transaparency%20Report%20July2016.pdf (includes requests via by court order and emergency requests).

real-time data.[35] T-Mobile, a service provider involved in *Carpenter*, 819 F.3d at 885, does not report requests for real-time location data specifically but received far more requests for customer data as a whole than its much larger rivals.[36]

III. Real-Time Cell Phone Tracking Presents Even Greater Privacy Concerns than the Technologies Considered in *Knotts*, *Karo*, *Kyllo*, and *Jones*.

Because real-time cell phone tracking gives the government the ability to locate any phone—and by extension the phone's owner—at any time and track it on an ongoing basis, it impacts two distinct privacy interests: privacy in one's location in the moment, and privacy in one's movements over time.

---

35. *See* AT&T, *AT&T Transparency Report* 4, 8 (2017), *available at* http://about.att.com/content/dam/csr/Transparency%20Reports/Feb-2017-Transparency-Report.pdf ("'Exigent requests' are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies.").

36. 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.

A. Because Cell Phones May Be Tracked Into Private Spaces and Reveal Individuals' Locations, the Fourth Amendment Applies.

Unlike a car, a cell phone regularly enters traditionally Fourth Amendment-protected spaces, like the home. For that reason, tracking the phone will reveal private information about a person's location in the moment that one could never learn by tracking a car. Because a phone's location is not limited to areas like "public thoroughfares" that are readily observable to the public, the Sixth Circuit's application of *Knotts* to real-time cell phone tracking is misplaced.

As the 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). This makes very real the possibility that cell phone tracking could allow law enforcement officers to find "the lady of the house" while she is taking "her daily sauna and bath—a [location] that many would consider 'intimate.'" *Kyllo*, 533 U.S. at 38; *see also Maryland Real-Time Order*, 849 F. Supp. 2d at 540 (noting "the precision of GPS and cell site location technology considered in combination with other factors demonstrates that [it] . . . will in many instances place the user within a home, or even a particular room of a home").

This Court has recognized that the Fourth Amendment draws a "firm" and a "bright" "line at the entrance to the house." *Kyllo*, 533 U.S. at 40 (citing *Payton v. New York*, 445 U.S. 573, 590 (1980)). Using a beeper to track someone into "a private residence, a location not open to

visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." *Karo*, 468 U.S. at 714. Similarly, using a thermal imaging device "to explore details of the home that would previously have been unknowable without physical intrusion . . . is a 'search' and is presumptively unreasonable without a warrant." *Kyllo*, 533 U.S. at 40.

The Sixth Circuit disregarded this precedent in *Skinner*. 690 F.3d at 780.[37] Instead, the court relied on *Knotts*, 460 U.S. at 281, to hold that individuals do not have a reasonable expectation of privacy in real-time location data created by their cell phones "voluntarily used while traveling on public thoroughfares." *Id.* at 779, 781.

However, this Court's subsequent decision in *Karo* demonstrates why reliance on *Knotts* is unworkable in this context. Both *Knotts* and *Karo* involved warrantless use of beepers hidden in containers of chemicals to track suspects' cars on public roads. *Knotts*, 460 U.S. at 278-79; *Karo*, 468 U.S. at 709-10. In *Knotts*, the police tracked a beeper hidden in a drum of chloroform in the suspect's car to a "secluded cabin," but they stopped monitoring once the "location in the area of the cabin had been initially determined." 460 U.S. at 277-79. The Court held that the suspect had no expectation of privacy in his movements on public streets because this information was "voluntarily conveyed to anyone who wanted to look." *Id.* at 281-82. In *Karo*, by contrast, the suspect carried a can of ether containing a beeper into a private house, and the police continued using the beeper to confirm that

37. In *Rios*, the Sixth Circuit cited, without further analysis, to its earlier opinion in *Skinner* to hold a warrant was not required to obtain real-time tracking information. 830 F.3d at 428.

the can remained in the house as vehicles came and went. 468 U.S. at 709-10. The Court held that this electronic surveillance violated the suspect's expectation of privacy because, unlike *Knotts,* it revealed "a critical fact about the interior of the premises that the Government [wa]s extremely interested in knowing and that it could not have otherwise obtained without a warrant." *Id.* at 715.

The Sixth Circuit incorrectly reasoned that the real-time cell phone tracking of the suspect in *Skinner* was akin to *Knotts* rather than *Karo*, because Skinner happened to be on public roads throughout the time he was tracked. 690 F.3d at 780-81. But as the Florida Supreme Court recognized in *Tracey*, which similarly involved tracking a suspect's phone in public: "because cell phones are indispensable to so many people and are normally carried on one's person, 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, is clearly a Fourth Amendment violation." 152 So. 3d at 524. Indeed, in *Karo* itself, this Court rejected the government's argument that it should not be required to seek a warrant because it had "no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises":

> We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device . . . whether a particular article—or a person, for that matter—is in an individual's home at a particular time.

468 U.S. at 716, 718.

The Sixth Circuit's "public thoroughfares" reasoning with respect to real-time cell phone tracking thus disregards the reality of how Americans use cell phones and creates an unworkable rule. Even where the government ends up tracking an individual's cell phone only in public spaces, it cannot ensure this result in advance. The Fourth Amendment requires "clear guidance to law enforcement through categorical rules," not the sort of case-by-case, post-hoc analysis invited by *Skinner*. *See Riley*, 134 S. Ct. at 2491; *see also Kyllo*, 533 U.S. at 38-39 (declining to draw Fourth Amendment line protecting only "intimate details" of the home because "no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details") (emphasis in original).

B. Real-Time Cell Phone Tracking Also Implicates Individuals' Expectation of Privacy in Their Movements Over Time.

Real-time cell phone tracking also impacts another distinct privacy interest recognized in *Jones*—namely privacy in one's movements over time. Although this case presents a relatively short time period of surveillance compared to *Jones*, that does not minimize the privacy concerns raised by warrantless cell phone tracking. As Justice Sotomayor noted, "[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance . . . will require particular attention." 565 U.S. at 415 (Sotomayor, J., concurring). This is because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* A person's movements over time

also reveal a wealth of information about expressive and associational activities protected by the First Amendment. *See Smith v. Maryland*, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting) (citing *NAACP v. Alabama*, 357 U.S. 449, 461 (1958)); *Roberts v. U.S. Jaycees*, 468 U.S. 609, 617-18 (1984).

Due to the invasive nature of real-time cell phone tracking, this Court should avoid the struggle to determine "with precision the point" at which tracking becomes a search. *Jones*, 565 U.S. at 430 (Alito J., concurring). As the Florida Supreme Court concluded in *Tracey*, "basing the determination as to whether warrantless real time cell site location tracking violates the Fourth Amendment on the length of the time the cell phone is monitored is not a workable analysis." 152 So. 3d at 520. Indeed, "where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant." *Jones*, 565 U.S.at 430 (Alito, J., concurring).

IV. The Third Party Doctrine Does Not Apply to Prospective Location Data.

The government has frequently relied on *Smith v. Maryland*, 442 U.S. 735, 744 (1979), to argue that cell phone users have no expectation of privacy in their location data. *See, e.g.*, *Carpenter*, 819 F.3d at 888 (no expectation of privacy in historical cell site location information because users voluntarily expose this data to cell providers); *Wallace*, 857 F.3d at 690 (no expectation of privacy in prospective location data because it is a business record transmitted to cell provider).

This "Third Party Doctrine" should not defeat an expectation of privacy in historical location data generated as a byproduct of using a cell phone.[38] Even if it did, the doctrine would have no applicability to *prospective* location data, which involves data created solely pursuant to government request. As discussed above, when a service provider receives a request to track a phone in real time, it obtains the phone's location by continuously "pinging" the device. This "pinging" is "not collected as a necessary part of cellular phone service, nor generated by the customer in placing or receiving a call." *Maryland Real-Time Order*, 849 F. Supp. 2d at 539 n.6. And it occurs even when no call is in process, without the phone owner's knowledge. *Id.* at 534. Under these circumstances, "it is difficult to understand how the user 'voluntarily' exposed such information to a third party." *Id.* at 539 n.6; *see also Tracey*, 152 So. 3d at 523 (requiring cell phone user to turn phone off to preserve expectation of privacy would be an "unreasonable burden").

The vast majority of location data generated by modern cell phones is thus created "with far less intent, awareness, or affirmative conduct on the part of the user than what was at issue in . . . *Smith*." *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1029. Such passive, unknowing generation of location information does not amount to a "voluntary conveyance" under the Third Party Doctrine. *Id; see also Tracey*, 152 So. 3d at 522 (rejecting notion that cellphone user's knowledge that "his cell phone gives off signals that enable the service provider to detect its location" means

38. *See* Br. of Amici Curiae Electronic Frontier Foundation et al., *Carpenter v. United States*, No. 16-402 (S. Ct. filed Oct. 28, 2016).

the user "is consenting to use of that location information by third parties for any other unrelated purposes").

CONCLUSION

Given the prevalence of cell phones and the quantity of law enforcement requests for real-time cell phone tracking, *Rios* presents questions of compelling national importance. The legal protections offered for cell phone tracking are not uniform, and courts have issued conflicting opinions on the issue, leaving the public and law enforcement in limbo. This Court should grant certiorari to clarify that the Fourth Amendment prohibits warrantless real-time cell phone tracking.

Dated: June 26, 2017

Respectfully submitted,

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

Attorneys for Amici Curiae

APPENDIX — LIST OF *AMICI CURIAE*

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 *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 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.

Appendix

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).