Case No. 12-12928

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff-Appellee,

v.

QUARTAVIOUS DAVIS,

Defendant-Appellant

On Appeal from the United States District Court
for the Southern District of Florida
The Honorable Joan A. Leonard
Case No. 1:10-cr-20896-JAL-2

EN BANC BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANT

Hanni Fakhoury
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
hanni@eff.org
jlynch@eff.org

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

United States v. Quartavious Davis
Case No. 12-12928

CERTIFICATE OF INTERESTED PERSONS

Pursuant to 11th Cir. R. 26.1-1, undersigned counsel for amicus curiae Electronic Frontier Foundation certifies that the following list includes all persons and entities having an interest in the outcome of this case, as well as all persons and entities listed on all certificates filed in the appeal prior to the filing date of this amicus curiae brief.

Agarwal, Amit

Altman, Roy

American Civil Liberties Union Foundation

American Civil Liberties Union Foundation of Florida, Inc.

Bankston, Kevin

Brown, Hon. Stephen T.

Caruso, Michael

Center for Democracy & Technology

Colan, Jonathan

Crump, Catherine

Davis, Quartavious

Dube, Hon. Robert L.

Electronic Frontier Foundation

United States v. Quartavious Davis
Case No. 12-12928

Fakhoury, Hanni

Ferrer, Wifredo A.

Fisher, Sylvester

Garber, Hon. Barry L.

Gold, Hon. Alan S.

Golembe, Stephen J.

Hayes, Anne M.

Kayanan, Maria

Korchin, Paul M.

Lenard, Hon. Joan A.

Lynch, Jennifer

Malone, Omar

Markus, Davis Oscar

Martin, Jahmal A.

Martin, Michael

Mayor's Jewelers

McAliley, Hon. Chris M.

Michaels, Alexander J.

United States v. Quartavious Davis
Case No. 12-12928

Moss, Jr., Reginald A.

National Association of Criminal Defense Lawyers

Nojeim, Greg

O'Sullivan, Hon. John J.

Palermo, Hon. Peter R.

Perwin, Amanda

Quencer, Kevin S.

Reid, Jamarquis T.

Salyer, Kathleen M.

Schultz, Anne R.

Shapiro, Jacqueline E.

Sibila, Jorge A.

Smith, Willie

Stevenson, Benjamin James

Torres, Hon. Edwin G.

Turnoff, Hon. William C

Ungaro, Hon. Ursula

Wessler, Nathan Freed

United States v. Quartavious Davis
Case No. 12-12928

White, Hon. Patrick A.

Williams, Hon. Kathleen M.

Wizner, Ben

Zelman, Michael

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amicus curiae Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of the stock of amicus.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Cases

State Statutes

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST OF AMICUS[1]

EFF is a member-supported civil liberties organization based in San Francisco, California and works to protect innovation, free speech, and privacy in the digital world. With more than 23,000 dues-paying members nationwide, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. As part of its mission, EFF has served as *amicus curiae* in landmark cases addressing Fourth Amendment issues raised by emerging technologies. *See, e.g., Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *City of Ontario v. Quon*, 560 U.S. 746 (2010).

EFF has particular expertise and interest in location-based tracking technologies such as GPS and the collection of cell-site tracking data, and has served as amicus in numerous federal and state cases involving historical cell site information, including this specific case. *See United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014); *In re Appl. of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *In re Appl. 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);

[1] No party's counsel authored this brief in whole or in part. No party or party's counsel contributed money that was intended to fund preparing or submitting the brief. No person—other than amicus curiae, its members, or its counsel—contributed money that was intended to fund preparing or submitting the brief. Counsel for Appellee United States does not oppose this motion. Counsel for Appellant Quartavious Davis consents to this motion.

Commonwealth v. Augustine, 4 N.E.3d 846 (2014); *United States v. Jones*, 908 F. Supp. 2d 203 (D.D.C. 2012). EFF has also been appointed to serve as amicus in a case involving a government application to obtain historical cell site data. *See In re Appl. of U.S. for an Order Authorizing Disclosure of Historical Cell Site Info. for Telephone No. [Redacted]*, --- F. Supp. 2d ---, 2014 WL 1395082 (D.D.C. April 17, 2014) (Facciola, M.J.).

STATEMENT OF THE ISSUE

Whether the government violated the Fourth Amendment when it obtained 67 days' worth of Defendant's cell phone location information without a warrant.

SUMMARY OF ARGUMENT

In the 35 years since the Supreme Court decided *Smith v. Maryland*, 442 U.S. 735 (1979), the capacity for technology to reveal unexpectedly detailed information about our lives has increased exponentially. Where, in *Smith*, the government recorded the numbers dialed and received on one phone at one location for three days, today the government can obtain not just those numbers but also all the locations the phone's owner traveled while the phone was able to make or receive a call. This technology was "nearly inconceivable just a few decades ago." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). As the Supreme Court recognized in *Kyllo v. United States*, given advances in technology, courts must

increasingly address "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. 27, 34 (2001).

Courts and legislatures across the country are responding to changing technologies by pushing beyond the case law of 35 years ago and recognizing greater privacy protections for the data—including location information—we store on our devices, in the "cloud," and with third parties. As more Americans have a subjective expectation of privacy in their location data, these expectations necessarily become ones that "society is prepared to recognize [are] 'reasonable,'" and thus protected by the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

The panel opinion below recognized this reality, finding "the exposure of the cell site location information [("CSLI")] can convert what would otherwise be a private event into a public one," thus triggering a Fourth Amendment reasonable expectation of privacy. *United States v. Davis*, 754 F.3d 1205, 1216 (11th Cir. 2014). The *en banc* court should affirm the panel opinion and require the government to use a probable cause search warrant to obtain historical CSLI.

ARGUMENT

I. AMERICANS HAVE A SUBJECTIVE EXPECTATION OF PRIVACY IN LOCATION INFORMATION.

Owning a cell phone is not a luxury; today more than 90%[2] of all American adults have a cell phone, and landline phones are becoming increasingly obsolete.[3] Cell phones generate a staggering amount of data about where the phone's owner has travelled throughout her daily life, including through CSLI. Society is increasingly recognizing that location data like this deserves "the most scrupulous protection from government invasion." *Oliver v. United States*, 466 U.S. 170, 178 (1984) (citation omitted).

Many federal and state courts have recognized an expectation of privacy in location and phone records generally and CSLI specifically. As more people live in states where these records are deemed private, the government cannot assert it is unreasonable to expect privacy in them. Thus, the panel was correct to require a probable cause search warrant to obtain CSLI.

---

[2] Pew Research Center, "Cell Phone Ownership Hits 91% of Adults," (June 6, 2013) http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

[3] *See* National Journal, "Americans Continue to Drop Their Landline Phones," (December 18, 2013) http://www.nationaljournal.com/hotline-on-call/americans-continue-to-drop-their-landline-phones-20131218 (citing CDC statistics finding 36.5% of U.S. adults live in household with no landline phone).

A. Research Shows Americans Believe the Data on and Generated by their Cell Phones is Private.

For the Fourth Amendment to apply, a person must have "exhibited an actual expectation of privacy." *Bond v. United States*, 529 U.S. 334, 338 (2000). Recent studies show Americans expect privacy in the data stored on and generated by their cell phones, including location information. Just this month, the Pew Research Center found 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.[4] In 2012, the Pew Center found that cell phone owners take a number of steps to protect access to their personal information and mobile data, and more than half of phone owners with mobile apps have uninstalled or decided to not install an app due to concerns about the privacy in their personal information.[5] In addition, more than 30% of smart phone owners polled took affirmative steps to safeguard their privacy: 19% turned off location tracking on their phones and 32% cleared their browsing or search history.[6] The numbers are higher for teenagers,

[4] Pew Research Center, "Public Perceptions of Privacy and Security in the Post-Snowden Era," 36-37 (Nov. 2014) http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (50% of respondents believed location information was "very sensitive").

[5] Pew Research Internet Project, "Privacy and Data Management on Mobile Devices," (Sept. 5, 2012) http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.

[6] *Id*.

with Pew reporting 46% of teenagers turned location services off.[7] A 2013 survey conducted on behalf of the Internet company TRUSTe found 69% of American smart phone users did not like the idea of being tracked.[8] And a 2009 Carnegie Mellon survey of perceptions about location-sharing technologies showed that participants believed the risks of location-sharing technologies outweighed the benefits and were "extremely concerned" about controlling access to their location information.[9]

These studies show Americans have a subjective expectation of privacy in their phone records and location information.

B. Courts Recognize the Privacy Implications of Location Information.

Given these statistics, it is unsurprising that courts around the country have also recognized the privacy implications of location information. In 2012, the Supreme Court suggested in *United States v. Jones*, that people expect their otherwise public movements on the street to remain private. 132 S. Ct. 945 (2012). Although the Court ultimately held that placing a GPS tracking device on a car was

[7] Pew Research Internet Project, "Location-Based Services" (Sept. 12, 2013) http://www.pewinternet.org/2013/09/12/location-based-services/.

[8] Truste, "TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size," (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/.

[9] Janice Y. Tsai, *et al*. "Location-Sharing Technologies: Privacy Risks and Controls," Carnegie Mellon University, 12 (Feb. 2010) http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

a "search" because it was a physical trespass onto private property, in two separate concurring opinions, five members of the Supreme Court recognized that location tracking could violate a reasonable expectation of privacy. Justice Sotomayor questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain . . . their political and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring). And Justice Alito wrote on behalf of three other justices, "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964 (Alito, J., concurring).[10]

In the wake of *Jones*, several state and federal courts—including, most recently, the Florida Supreme Court—have recognized the privacy implications of location information and historical CSLI specifically. In protecting historical cell site data in *Commonwealth v. Augustine*, the Massachusetts Supreme Judicial Court—like the panel below in this case—recognized that this data may raise even greater privacy concerns than GPS tracking devices placed on a car because cell

[10] Earlier this year, the Supreme Court in *Riley v. California* specifically cited Justice Sotomayor's concurring opinion in *Jones* as a reason to limit police searches of cell phones incident to arrest. 134 S. Ct. at 2490. *Riley* recognized the privacy implications of location information, noting that cell phones store data that can "reveal where a person has been," making it possible to "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

site data can track "the user's location far beyond the limitations of where a car can travel"—including into "constitutionally protected areas" like a home. 4 N.E. 3d 846, 861-62 (Mass. 2014); *see also Davis*, 754 F.3d at 1216 ("while it may be the case that even in light of the *Jones* opinion, GPS location information on an automobile would be protected only in the case of aggregated data, even one point of cell site location data can be within a reasonable expectation of privacy"). *Augustine* also noted historical cell site data gave police access to something it would never have with traditional law enforcement investigative methods: the ability "to track and reconstruct a person's past movements." *Id.* at 865.

Similarly, in *State v. Earls*, the New Jersey Supreme Court noted users should be "entitled to expect confidentiality in the ever-increasing level of detail that cell phones can reveal about their lives" and adopted a warrant requirement for historical CSLI. 70 A.3d 630, 644 (N.J. 2013). And just last month, the Florida Supreme Court noted "the close relationship an owner shares with his cell phone" makes "a cell phone's movements its owner's movements." *Tracey v. State*, --- So.3d ---, 2014 WL 5285929, *18, (Fla. 2014). The court found a subjective expectation of privacy "in the location signals transmitted solely to enable the private and personal use of his cell phone, even on public roads." *Id.* at *19**.**

II. AN EXPECTATION OF PRIVACY IN CELL PHONE DATA IS OBJECTIVELY REASONABLE EVEN THOUGH THE DATA IS HELD BY A PHONE COMPANY.

This subjective expectation of privacy in CSLI is not defeated simply because this location information is exposed to the telephone company. Before the panel, the government relied on *Smith* to argue cell phone users have no expectation of privacy in historical CSLI because that data has been exposed to a third party. *See Davis*, 754 F.3d at 1216 (citing *Smith*, 442 U.S. at 742-44). According to the government, when a person voluntarily uses a cell phone, she knows the phone is sending information about her location to the phone company and thus cannot expect the phone company to keep that information private. But *Smith* does not alter the calculus here for two reasons.

First, the data here is significantly more revealing than the limited three days worth of call records at issue in *Smith*. The Supreme Court in *Riley v. California* recognized that cell phones store "qualitatively different" types of data compared to physical records and noted that because today's advanced technology can disclose much more revealing personal information than technologies of the past, the "scope of the privacy interests at stake" far exceeds that of any analogue in the physical world. 134 S. Ct. at 2490, 2491. Although, the government argued in *Riley* that cellphones are "materially indistinguishable" from physical items that may be searched without a warrant incident to arrest like the pack of cigarettes at issue in

United States v. Robinson, 414 U.S. 218, 236 (1973), the Court refused to equate the two. *Riley*, 134 S. Ct. at 2488-89. It believed comparing a search of all data on a cell phone to the search of physical items is "like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 134 S. Ct. at 2488.

Similarly, here, because the data generated by CSLI is so different in quantity and quality from the data generated by a simple landline phone, this Court cannot rely only on antiquated cases to determine how to protect cell phone data, especially data that reveals sensitive location information. *Id*. at 2488-89. This Court has already recognized that "whether the analytical framework, much less the rationale" of *Smith* applies to modern technologies "is questionable and far from clearly established." *Rehberg v. Paulk*, 611 F.3d 828, 847 (11th Cir. 2010). Instead, this Court should look to actual societal understandings of privacy in cell phone data and location information to determine the protections necessary to satisfy the Fourth Amendment.

Second, *Smith* does not reflect the realities of modern society. Today we share much more information about ourselves with third parties merely as a byproduct of the differences in how we perform tasks today versus in the past—whether it is writing emails instead of letters; collaborating on document drafting

online instead of through hard-copy printouts, or buying and reading books on our phones or Kindles versus purchasing a physical book at a bookstore to read later in the privacy of our own homes. As Justice Sotomayor noted in *Jones*, *Smith*'s basic "premise" is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). Honing in on subjective expectations of privacy, Justice Sotomayor doubted "people would accept without complaint the warrantless disclosure" of information to the government like URLs they visit or the phone numbers they dial or text. *Id.*

Other courts have reached the same conclusions, both before and after *Jones*, finding expectations of privacy in data stored by third parties, including emails stored on a service provider's servers, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); patient prescription records stored in an online database, *Oregon Prescription Drug Monitoring Program v. DEA*, 998 F. Supp. 2d 957 (D. Ore. 2014); and even CSLI itself. *Augustine*, 4 N.E.3d at 850; *Earls*, 70 A.3d at 644. This includes the Florida Supreme Court, which has found an expectation of privacy in real-time CSLI notwithstanding *Smith* in part because cell phones are so "indispensable" that "cell phone tracking can easily invade the right to privacy in

one's home or other private areas." *Tracey*, 2014 WL 5285929 at *17.[11] *Tracey* noted a person did not "voluntarily convey that information to the service provider for any purpose other than to enable use of his cell phone for its intended purpose" and rejected the "fiction" that people consent to warrantless cell phone tracking as a condition of carrying a cell phone. *Id.* at *17, *19.

For this reason, the government's argument that cell phone users—especially those within this Court's jurisdiction in Florida—cannot expect location information to remain private once the data has been exposed to the phone company is incorrect. On the contrary, at a minimum all Floridians have been promised that, because cell phone data reveals detailed personal information, cell phone customers have a reasonable expectation of privacy in that data, even though it is held by a third party. *Tracey*, 2014 WL 5285929 at *17. Ultimately, that means *Smith* does not control the outcome of this case. Just because technology is *capable* of disclosing what is otherwise private information about a person's specific location does not mean that a person has a lesser expectation of privacy under the Fourth Amendment.

[11] The Court in *Tracey* analyzed the issue solely under the Fourth Amendment. *See Tracey*, 2014 WL 5285929 at *5. But earlier Florida Supreme Court cases interpreting Florida's state constitution have also rejected *Smith* to find an expectation of privacy in phone and banking records, even though those records are held by a third party. *See State v. Shaktman*, 553 So.2d 148 (Fla. 1989) (expectation of privacy in phone records); *Winfield v. Div. of Pari-Mutuel Wagering, Dep't of Bus. Regulation*, 477 So.2d 544 (Fla. 1985) (expectation of privacy in banking records).

III. THE NATIONWIDE TREND TOWARD GREATER PROTECTION FOR PRIVACY IN PHONE RECORDS AND LOCATION INFORMATION SHOWS SOCIETY RECOGNIZES THAT A PRIVACY INTEREST IN THIS DATA IS REASONABLE.

Having established that people generally have a subjective expectation of privacy in their location, that advances in technology require changes in legal analyses, and that Floridians specifically have an expectation of privacy in phone records, the question remains whether broader society is prepared to recognize that subjective expectation of privacy as reasonable. The answer is yes.

A court reviewing the appropriate Fourth Amendment limits to be placed on searches must necessarily look to "societal understandings" of what should be considered private to determine reasonable expectations of privacy. *Oliver*, 466 U.S. at 178; *see also United States v. Brown*, 743 F.2d 1505, 1507 (11th Cir. 1984). Further, while the Fourth Amendment is not "a redundant guarantee of whatever limits on search and seizure legislatures might have enacted," *Virginia v. Moore*, 553 U.S. 164, 168 (2008), the existence of both federal and state statutory protection for certain kinds of information helps inform whether society has determined that a particular expectation of privacy is reasonable. *See, e.g., United States v. Maynard*, 615 F.3d 544, 564 (D.C. Cir. 2010) ("state laws are indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable"); *Doe v. Broderick*, 225 F.3d 440, 450 (4th Cir. 2000) (federal statutory protection "is relevant to the determination of whether there is a

'societal understanding'" of a legitimate expectation of privacy in medical records); *United States v. Nerber*, 222 F.3d 597, 604-05 (9th Cir. 2000) (federal wiretap statute is "strong evidence" that society would find warrantless video surveillance unreasonable).

The societal recognition of privacy in phone records and location information is reflected in federal and state cases and state statutes deeming this data to be private. After *Smith* was decided, courts in California, Colorado, Hawaii, Idaho, Illinois, New Jersey, Pennsylvania, Washington and Florida all rejected *Smith*, finding those states' residents had a reasonable expectation of privacy under their state constitutions in dialed phone numbers—notwithstanding the fact those records are held by the phone provider.[12] By statute, Georgia and Oregon required police to demonstrate probable cause to install and operate a pen register to obtain dialed phone numbers.[13]

---

[12] *See People v. Blair*, 602 P.2d 738, 746 (Cal. 1979); *People v. Sporleder*, 666 P.2d 135, 141-43 (Colo. 1983); *State v. Rothman*, 779 P.2d 1, 7-8 (Haw. 1989); *State v. Thompson*, 760 P.2d 1162, 1165-67 (Id. 1988); *People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill.Ct.App. 1993); *State v. Hunt*, 450 A.2d 952, 955-57 (N.J. 1982); *Commonwealth v. Melilli*, 555 A.2d 1254, 1256-59 (Pa. 1989); *State v. Gunwall*, 720 P.2d 808, 813-17 (Wash. 1986); *State v. Shaktman*, 553 So.2d 148 (Fla. 1989); *see generally* Stephen E. Henderson, *Learning From all Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

[13] *See Ellis v. State*, 353 S.E.2d 19, 21-22 (Ga. 1987) (pen register is "device" under Ga. Code Ann. § 16-11-64(b) whose installation requires probable cause search warrant); O.R.S. § 165.663.

Then, as technology continued to advance but before *Jones* was decided, the state supreme courts of New York, Oregon, and Washington held that people could reasonably expect privacy in their location, meaning that using technology to track a person's movements was a Fourth Amendment "search."[14] Five state legislatures passed statutes requiring police to obtain a probable cause search warrant to track a person's location with a tracking device like a GPS—even when the person is traveling in public places.[15] This meant that even before the Supreme Court addressed the question of whether Americans have a reasonable expectation of privacy in their location information, seven states—representing nearly 20% of the United States population[16]—already recognized this privacy right.

After *Jones*, the number of people across the country reasonably expecting privacy in their location has increased, as more courts have recognized that an expectation of privacy in a person's location means technologies like GPS or real-time cell phone tracking are Fourth Amendment "searches" under *Katz*.[17] That

---

[14] *See, e.g., People v. Weaver*, 909 N.E.2d 1195, 1201 (N.Y. 2009) (GPS); *State v. Campbell*, 759 P.2d 1040, 1048-49 (Or. 1988) (use of radio transmitter to locate automobile); *State v. Jackson*, 76 P.3d 217, 223-24 (Wash. 2003) (GPS).

[15] *See* Haw. Rev. Stat. § 803-44.7(b); Okla. Stat. Ann. tit. 13, § 177.6(A); Or. Rev. Stat. Ann. § 133.619(6); 18 Pa. Cons. Stat. Ann. § 5761(c)(4); S.C. Code Ann. § 17-30-140(b)(2).

[16] This figure is based on 2013 population data for each state, as projected by the U.S. Census. *See* United States Census Bureau, "Quick Facts," http://quickfacts.census.gov/qfd/index.html.

[17] *Commonwealth v. Rousseau*, 990 N.E.2d 543, 552-53 (Mass. 2013) (GPS); *Commonwealth v. Rushing*, 71 A.3d 939, 961-64 (Pa. Sup. Ct. 2013), *appeal*

includes the Florida Supreme Court's decision in *Tracey*, discussed above, which requires police to obtain a search warrant to track a cell phone's location in real time. *Tracey*, 2014 WL 5285929 at *19-20.

Courts and state legislatures have also extended privacy protections to historical CSLI. The high courts in Massachusetts and New Jersey—relying in part on Justice Sotomayor's concurrence in *Jones*—recognized a reasonable expectation of privacy in historical CSLI under their respective state constitutions and required police use a search warrant to obtain that information. *Augustine*, 4 N.E.3d at 850; *Earls*, 70 A.3d at 644. Five more states legislated privacy protections for historical cell site data, with Colorado, Maine, Minnesota, Montana and Utah passing statutes expressly requiring law enforcement to apply for a search warrant to obtain this data.[18]

In sum, the number of people in the United States—and in Florida specifically—who have been promised by court decision or legislation that information about where they have been is private has never been higher. The

---

granted on other grounds 84 A.3d 699 (2014) (cell phone signal); *State v. Brereton*, 826 N.W.2d 369, 379 (Wis. 2013) (GPS); *United States v. Powell*, 943 F. Supp. 2d 759, 776-77 (E.D. Mich. 2013) (real time cell site tracking); *State v. Zahn*, 812 N.W.2d 490, 496-499 (S.D. 2012) (GPS); *United States v. Lopez*, 895 F. Supp. 2d 592, 602 (D. Del. 2012) (GPS).

[18] *See* Colo. Rev. Stat. Ann. § 16-3-303.5(2); 16 Maine Rev. Stat. Ann. § 648; Minn. Stat. Ann. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); Utah Code Ann. § 77-23c-102(1)(a). A number of states have passed laws requiring police obtain a search warrant only to track a cell phone in real time. *See, e.g.,* Ind. Code 35-33-5-12; Wis. Stat. Ann. § 968.373(2).

growing number of people protected by the warrant requirement, while not dispositive of whether there is a Fourth Amendment expectation of privacy in historical CSLI, is compelling proof of "societal understandings" as to what level of privacy and security is reasonable. Thus the panel's decision should be affirmed.

CONCLUSION

For more than 90% of Americans, a cell phone is the only phone they have. As anyone who moves about in society recognizes, cell phones are constantly in use in both public and private spaces. At the same time, they are also "constantly connecting to cell sites, and those connections are recorded" by cell phone companies. *Augustine*, 4 N.E.3d at 860. This means that Americans are constantly and automatically generating an almost unfathomable wealth of information about their whereabouts.

When it comes to historical cell site records, it is clear that Americans generally, and Floridians specifically, expect that the location information revealed by these records remain private. Given the trend in legislatures and courts across the country to protect this privacy interest by requiring a warrant, society understands this expectation of privacy is reasonable.

This Court should follow the Supreme Court's lead in *Riley v. California* and recognize that, given the vast amount of data generated by cell phones, coupled with the trend toward greater privacy protections for that data, outdated

cases cannot govern the outcome here. Americans have a reasonable expectation of privacy in the location data generated by CSLI, and, as the Court noted in *Riley*, the answer to the question of what police must do before they may obtain that data is "simple—get a warrant." 134 S. Ct. at 2495.

Dated: November 17, 2014

Respectfully submitted,

/s/ Hanni Fakhoury

Hanni Fakhoury
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amicus Curiae* In Support Of Party-of-Interest-Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,228 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: November 17, 2014

Respectfully submitted,

/s/ Hanni Fakhoury
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Eleventh Circuit by using the appellate CM/ECF system on November 17, 2014.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: November 17, 2014

Respectfully submitted,

/s/ Hanni Fakhoury
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION