

1 Jennifer Lynch (SBN 240701)  
jlynch@eff.org  
2 Hanni M. Fakhoury (SBN 252629)  
hanni@eff.org  
3 ELECTRONIC FRONTIER FOUNDATION  
815 Eddy Street  
4 San Francisco, CA 94109  
Telephone: (415) 436-9333  
5 Facsimile: (415) 436-9993  
6 Counsel for *Amicus Curiae*  
ELECTRONIC FRONTIER FOUNDATION  
7

8  
9 **UNITED STATES DISTRICT COURT**  
10 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**  
11 **SAN FRANCISCO DIVISION**  
12

13  
14 IN RE TELEPHONE INFORMATION  
15 NEEDED FOR A CRIMINAL  
16 INVESTIGATION  
17

) Case No.: 3:14-xr-90532-NC-1

) **BRIEF *AMICUS CURIAE* OF**  
) **ELECTRONIC FRONTIER**  
) **FOUNDATION IN SUPPORT OF A**  
) **WARRANT REQUIREMENT FOR**  
) **HISTORICAL CELL SITE**  
) **INFORMATION**

) Courtroom A, 15<sup>th</sup> Floor  
) Hon. Nathanael Cousins  
18  
19  
20

**TABLE OF CONTENTS**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

INTRODUCTION..... 1

ARGUMENT ..... 1

    I.    AMERICANS HAVE AN EXPECTATION OF PRIVACY IN THE  
          LOCATION INFORMATION GENERATED BY THEIR CELL PHONES..... 1

        A.    Research Shows Americans Have a Subjective Expectation of Privacy in  
              the Data Generated by Their Cell Phones. .... 3

        B.    Courts Recognize the Privacy Implications of Location Information..... 4

    II.   THE “THIRD-PARTY DOCTRINE” DOES NOT CHANGE THE  
          EXPECTATION OF PRIVACY IN HISTORICAL CELL SITE  
          INFORMATION..... 6

    III.  THE NATIONWIDE TREND TOWARD GREATER PROTECTION FOR  
          PRIVACY IN PHONE RECORDS AND LOCATION INFORMATION SHOWS  
          SOCIETY RECOGNIZES A PRIVACY INTEREST IN THIS DATA IS  
          REASONABLE..... 9

CONCLUSION ..... 12

**TABLE OF AUTHORITIES**

**Cases**

1

2

3 *Bond v. United States,*

4 529 U.S. 334 (2000) ..... 3

5 *California v. Greenwood,*

6 486 U.S. 35 (1988) ..... 2

7 *Doe v. Broderick,*

8 225 F.3d 440 (4th Cir. 2000) ..... 3

9 *In re Application of the U.S. for Historical Cell Site Data,*

10 724 F.3d 600 (5th Cir. 2013) ..... 11

11 *In re Application of U.S. for an Order Directing a Provider of Electronic Communication*

12 *Service to Disclose Records,*

13 620 F.3d 304 (3d Cir. 2010) ..... 11

14 *Johnson v. United States,*

15 333 U.S. 10 (1948) ..... 2

16 *Katz v. United States,*

17 389 U.S. 347 (1967) ..... 1, 10

18 *Kyllo v. United States,*

19 533 U.S. 27 (2001) ..... 1

20 *Oliver v. United States,*

21 466 U.S. 170 (1984) ..... 2

22 *Payton v. New York,*

23 445 U.S. 573 (1980) ..... 2

24 *Rakas v. Illinois,*

25 439 U.S. 128 (1978) ..... 2

26 *Riley v. California,*

27 134 S. Ct. 2473 (2014) ..... *passim*

28 *Smith v. Maryland,*

442 U.S. 735 (1979) ..... *passim*

*Trujillo v. City of Ontario,*

428 F. Supp. 2d 1094 (C.D. Cal. 2006) ..... 3

*United States v. Davis,*

--- F.3d ---, 2014 WL 2599917 (11th Cir. 2014) ..... 5, 11, 12

1 *United States v. Forrester*,  
2 512 F.3d 500 (9th Cir. 2007) ..... 11, 12

3 *United States v. Golden Valley Elec. Ass'n*,  
4 689 F.3d 1108 (9th Cir. 2012) ..... 3

5 *United States v. Jones*,  
6 132 S. Ct. 945 (2012) ..... 4, 5, 9, 10

7 *United States v. Lopez*,  
8 895 F. Supp. 2d 592 (D. Del. 2012) ..... 10

9 *United States v. Maynard*,  
10 615 F.3d 544 (D.C. Cir. 2010)..... 2

11 *United States v. Miller*,  
12 425 U.S. 435 (1976) ..... 8

13 *United States v. Nerber*,  
14 222 F.3d 597 (9th Cir. 2000) ..... 3

15 *United States v. Powell*,  
16 943 F. Supp. 2d 759 (E.D. Mich. 2013) ..... 10

17 *United States v. Robinson*,  
18 414 U.S. 218 (1973) ..... 6

19 *United States v. Taketa*,  
20 923 F.2d 665 (9th Cir. 1991) ..... 3

21 *United States v. Velasquez*,  
22 No. CR-08-0730-WHA, 2010 WL 4286276 (N.D. Cal. Oct. 22, 2010) ..... 2

23 *Virginia v. Moore*,  
24 553 U.S. 164 (2008) ..... 2

21 **State Cases**

22 *Burrows v. Super. Ct.*,  
23 13 Cal.3d 238 (1974) ..... 8

24 *Commonwealth v. Augustine*,  
25 4 N.E. 3d 846 (Mass. 2014)..... 5, 6, 11, 12

26 *Commonwealth v. Melilli*,  
27 555 A.2d 1254 (Pa. 1989)..... 9

28 *Commonwealth v. Rousseau*,  
990 N.E.2d 543 (Mass. 2013)..... 10

1        *Commonwealth v. Rushing*,  
2            71 A.3d 939 (Pa. Sup. Ct. 2013),  
3            *appeal granted on other grounds* 84 A.3d 699 (2014)..... 10

4        *Ellis v. State*,  
5            353 S.E.2d 19 (Ga. 1987) ..... 9

6        *People v. Blair*,  
7            25 Cal. 3d 640 (Cal. 1979) ..... 7, 8

8        *People v. Chapman*,  
9            36 Cal. 3d 98 (1984),  
10           *disapproved on other grounds in People v. Palmer*, 24 Cal. 4th 856 (2001) ..... 7

11       *People v. DeLaire*,  
12           610 N.E.2d 1277 (Ill.Ct.App. 1993)..... 9

13       *People v. McKunes*,  
14           51 Cal. App. 3d 487, 492 (1975) ..... 7

15       *People v. Sporleder*,  
16           666 P.2d 135 (Colo. 1983) ..... 9

17       *People v. Weaver*,  
18           909 N.E.2d 1195 (N.Y. 2009) ..... 9

19       *Shaktman v. State*,  
20           553 So.2d 148 (Fla. 1989) ..... 9

21       *State v. Brereton*,  
22           826 N.W.2d 369 (Wis. 2013) ..... 10

23       *State v. Campbell*,  
24           759 P.2d 1040 (Or. 1988) ..... 9

25       *State v. Earls*,  
26           70 A.3d 630 (N.J. 2013) ..... 5, 13

27       *State v. Gunwall*,  
28           720 P.2d 808 (Wash. 1986) ..... 9

*State v. Hunt*,  
          450 A.2d 952 (N.J. 1982) ..... 9

*State v. Jackson*,  
          76 P.3d 217 (Wash. 2003) ..... 9

*State v. Rothman*,  
          779 P.2d 1 (Haw. 1989)..... 9

1     *State v. Thompson*,  
        760 P.2d 1162 (Id. 1988).....9

2     *State v. Walton*,  
        324 P.3d 876 (Haw. 2014)..... 11

3

4     *State v. Zahn*,  
        812 N.W.2d 490 (S.D. 2012)..... 10

5

6                                   **Federal Statutes**

7     18 U.S.C. §§ 3122-3127 ..... 7, 8

8                                   **State Statutes**

9     16 Maine Rev. Stat. Ann. § 648 ..... 13

10    18 Pa. Cons. Stat. Ann. § 5761(c)(4)..... 10

11    Haw. Rev. Stat. § 803-44.7(b).....9

12    Colo. Rev. Stat. Ann. § 16-3-303.5(2) ..... 13

13    Ind. Code 35-33-5-12 ..... 14

14    Minn. Stat. Ann. §§ 626A.28(3)(d), 626A.42(2) (effective August 1, 2014) ..... 13

15    Mont. Code Ann. § 46-5-110(1)(A) ..... 13

16

17    O.R.S. § 165.663 .....9

18    Okla. Stat. Ann. tit. 13, § 177.6(A) .....9

19    Or. Rev. Stat. Ann. § 133.619(6)..... 10

20    S.C. Code Ann. § 17-30-140(b)(2)..... 10

21    Utah Code Ann. § 77-23c-102(1)(a) ..... 13

22    Wisc. Stat. Ann. § 968.373(2) ..... 14

23                                   **Federal Constitutional Provisions**

24    U.S. Const., amend. IV .....*passim*

25                                   **State Constitutional Provisions**

26    Calif. Const., Art. I, section 13 ..... 10

27

28

**State Legislative Materials**

1  
2 69 Ops. Cal. Atty. Gen 55 (1986)..... 10  
3 86 Ops. Cal. Atty. Gen. 198 (2003)..... 11

**Other Authorities**

4  
5 Janice Y. Tsai, *et al.*, “Location-Sharing Technologies: Privacy Risks and Controls,” Carnegie  
6 Mellon University, 12 (Feb. 2010) [http://cups.cs.cmu.edu/LBSprivacy/files/  
TsaiKelleyCranorSadeh\\_2009.pdf](http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf) ..... 4  
7 National Journal, “Americans Continue to Drop Their Landline Phones,” (December 18, 2013)  
8 [http://www.nationaljournal.com/hotline-on-call/americans-continue-to-drop-their-  
landline-phones-20131218](http://www.nationaljournal.com/hotline-on-call/americans-continue-to-drop-their-landline-phones-20131218) ..... 1  
9 Pew Research Center, “Cell Phone Ownership Hits 91% of Adults,” (June 6, 2013)  
10 [http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-  
11 adults/](http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/) ..... 1  
12 Pew Research Internet Project, “Location-Based Services” (Sept. 12, 2013)  
13 <http://www.pewinternet.org/2013/09/12/location-based-services/>..... 4  
14 Pew Research Internet Project, “Privacy and Data Management on Mobile Devices,” (Sept. 5,  
15 2012) [http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-  
mobile-devices/](http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/)..... 4  
16 Stephen E. Henderson, *Learning From all Fifty States: How to Apply the Fourth Amendment  
17 and its State Analogs to Protect Third Party Information from Unreasonable Search*,  
55 Cath. U. L. Rev. 373 (2006) ..... 9  
18 Truste, “TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy  
19 Than Brand or Screen Size,” (Sept. 5, 2013)  
20 [http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-  
concerned-about-mobile-privacy-than-brand-or-screen-size/](http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size/) ..... 4  
21 United States Census Bureau, “Quick Facts,” <http://quickfacts.census.gov/qfd/index.html> ..... 10  
22  
23  
24  
25  
26  
27  
28

1 **INTRODUCTION**

2 In the more than 35 years since the Supreme Court decided *Smith v. Maryland*, 442 U.S.  
3 735 (1979), the capacity for technology to reveal unexpectedly detailed information about our lives  
4 has increased exponentially year after year. Where, in *Smith*, the government was able to record the  
5 numbers dialed and received on one phone at one location for three days, now the government can  
6 obtain not just those numbers but also information about all the locations where the phone's owner  
7 traveled during the entire time the phone was capable of receiving or making a call. This  
8 technology was "nearly inconceivable just a few decades ago." *Riley v. California*, 134 S. Ct. 2473,  
9 2484 (2014). As the Supreme Court recognized in *Kyllo v. United States*, given these advances in  
10 technology, courts must increasingly face the question of "what limits there are upon this power of  
11 technology to shrink the realm of guaranteed privacy." 533 U.S. 27, 34 (2001).

12 Courts and legislatures across the country are responding by pushing beyond the case law  
13 of 35 years ago and enacting greater privacy protections for the data we store on our technical  
14 devices, in the "cloud," and with third parties. As more Americans have a subjective expectation of  
15 privacy in their data, these expectations necessarily become ones that "society is prepared to  
16 recognize [are] 'reasonable,'" and thus protected by the Fourth Amendment. *Katz v. United States*,  
17 389 U.S. 347, 361 (1967) (Harlan, J., concurring). This Court should follow this clear trend and  
18 require the government to use a probable cause search warrant to obtain historical cell site records.

19 **ARGUMENT**

20 **I. AMERICANS HAVE AN EXPECTATION OF PRIVACY IN THE LOCATION**  
21 **INFORMATION GENERATED BY THEIR CELL PHONES.**

22 Owning a cell phone is not a luxury; today more than 90%<sup>1</sup> of all American adults have a  
23 cell phone, and landline phones are becoming increasingly obsolete.<sup>2</sup> Through historical cell site

24 \_\_\_\_\_  
25 <sup>1</sup> 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/>.

26 <sup>2</sup> See National Journal, "Americans Continue to Drop Their Landline Phones," (December 18,  
27 2013) <http://www.nationaljournal.com/hotline-on-call/americans-continue-to-drop-their-landline-phones-20131218> (citing CDC statistics finding 38% of U.S. adults live in household with no  
28 landline phone).



1 information—the records of which cell phone towers a cell phone customer connects to and  
2 when—these cell phones generate a staggering amount of data about where the cell phone’s owner  
3 has travelled throughout her daily life—data that is available to law enforcement.

4 Society is increasingly recognizing that location data like this deserves “the most  
5 scrupulous protection from government invasion.” *Oliver v. United States*, 466 U.S. 170, 178  
6 (1984) (citing *Payton v. New York*, 445 U.S. 573 (1980)). A court reviewing the appropriate Fourth  
7 Amendment limits to be placed on searches of and by new technologies must necessarily look to  
8 “societal understandings” of what should be considered private to determine what privacy  
9 expectations are reasonable. *Oliver*, 466 U.S. at 178; *see also Rakas v. Illinois*, 439 U.S. 128, 143  
10 n. 12 (1978) (Fourth Amendment “expectation of privacy” must “have a source outside of the  
11 Fourth Amendment” by referencing “understandings that are recognized and permitted by  
12 society.”). That ensures the Fourth Amendment remains a manifestation of society’s belief that it  
13 chooses “to dwell in reasonable security and freedom from surveillance.” *Johnson v. United States*,  
14 333 U.S. 10, 14 (1948).

15 This societal recognition of privacy in historical cell site information and other telephone  
16 records is reflected in recent federal and state cases and statutes deeming this data to be private.  
17 While, the Fourth Amendment is not dependent on any specific state’s laws, *see California v.*  
18 *Greenwood*, 486 U.S. 35, 43 (1988), federal courts have not hesitated to look to state law to  
19 determine whether an expectation of privacy is reasonable. *See United States v. Maynard*, 615 F.3d  
20 544, 564 (D.C. Cir. 2010) (“state laws are indicative that prolonged GPS monitoring defeats an  
21 expectation of privacy that our society recognizes as reasonable”); *see also United States v.*  
22 *Velasquez*, No. CR-08-0730-WHA, 2010 WL 4286276, \*5 (N.D. Cal. Oct. 22, 2010) (unpublished)  
23 (“the recognition of a privacy right by numerous states may provide insight into broad societal  
24 expectations of privacy”).

25 Similarly, while the Fourth Amendment is not “a redundant guarantee of whatever limits on  
26 search and seizure legislatures might have enacted,” *Virginia v. Moore*, 553 U.S. 164, 168 (2008),  
27 the existence of both federal and state statutory protection for certain kinds of information helps

1 inform whether society has determined that a particular expectation of privacy is reasonable. *See,*  
2 *e.g., United States v. Nerber*, 222 F.3d 597, 604-05 (9th Cir. 2000) (federal wiretap statute is  
3 “strong evidence” that society would find warrantless video surveillance unreasonable); *Doe v.*  
4 *Broderick*, 225 F.3d 440, 450 (4th Cir. 2000) (federal statutory protection “is relevant to the  
5 determination of whether there is a ‘societal understanding’” of a legitimate expectation of privacy  
6 in medical records); *Trujillo v. City of Ontario*, 428 F. Supp. 2d 1094, 1106 (C.D. Cal. 2006)  
7 (California statutes governing video surveillance in locker rooms and restrooms represent  
8 “society’s understanding that a locker room is a private place” under the Fourth Amendment).<sup>3</sup>

9 Many state courts and legislatures, including the California Supreme Court, have  
10 recognized an expectation of privacy in location and phone records generally, and historical cell  
11 site information specifically. As more people live in states where these records are considered  
12 private, the government can no longer assert it is unreasonable to expect privacy in them. Thus, a  
13 probable cause search warrant is necessary to obtain historical cell site records.

14 **A. Research Shows Americans Have a Subjective Expectation of Privacy in the**  
15 **Data Generated by Their Cell Phones.**

16 For the Fourth Amendment to apply, a person must have an actual “expectation that his  
17 activities would be private.” *Nerber*, 222 F.3d at 599 (citing *Bond v. United States*, 529 U.S. 334,  
18 338 (2000). “Privacy does not require solitude,” *United States v. Taketa*, 923 F.2d 665, 673 (9th  
19 Cir. 1991), and even when a person “cannot expect total privacy,” he may nonetheless have an  
20 expectation of privacy from intrusions going beyond what he may otherwise anticipate. *Nerber*,  
21 222 F.3d at 604.

22 Recent studies show Americans have an expectation of privacy in the data stored on and  
23 generated by their cell phones, including location information. In 2012, the Pew Research Center  
24 found that cell phone owners take a number of steps to protect access to their personal information  
25 and mobile data, and more than half of phone owners with mobile apps have uninstalled or decided

26 <sup>3</sup> The Ninth Circuit has even suggested that “a company’s guarantee to its customers that it will  
27 safeguard the privacy of their records might suffice to justify resisting an administrative subpoena”  
28 in lieu of a warrant to obtain certain records. *United States v. Golden Valley Elec. Ass’n*, 689 F.3d  
1108, 1116 (9th Cir. 2012).

1 to not install an app due to concerns about the privacy in their personal information. In addition,  
2 more than 30% of smart phone owners polled took affirmative steps to safeguard their privacy:  
3 19% turned off location tracking on their phones and 32% cleared their browsing or search  
4 history.<sup>4</sup> The numbers are higher for teenagers, with Pew reporting 46% of teenagers turned  
5 location services off.<sup>5</sup> A 2013 survey conducted on behalf of the Internet company TRUSTe found  
6 69% of American smart phone users did not like the idea of being tracked.<sup>6</sup> And a 2009 Carnegie  
7 Mellon survey of perceptions about location-sharing technologies showed that participants believed  
8 the risks of location-sharing technologies outweighed the benefits and were “extremely concerned”  
9 about controlling access to their location information.<sup>7</sup>

10 **B. Courts Recognize the Privacy Implications of Location Information.**

11 Gauging public apprehension about technologies shrinking privacy, an increasing number  
12 of courts across the country have recognized the privacy implications of location information. In  
13 2012, the Supreme Court suggested in *United States v. Jones* that people expect their otherwise  
14 public movements on the street to remain private. 132 S. Ct. 945 (2012). Although the Court  
15 ultimately ruled placing a GPS tracking device on a car was a “search” because it was a physical  
16 trespass onto private property, in two separate concurring opinions, five members of the Supreme  
17 Court expressed concern that technology could intrude upon expectations of privacy. Critically, the  
18 concurring opinions of both Justice Sotomayor and Justice Alito (joined by four other justices)  
19 doubted that people reasonably expect their public movements would be monitored extensively.  
20 Justice Sotomayor questioned “whether people reasonably expect that their movements will be  
21 recorded and aggregated in a manner that enables the Government to ascertain . . . their political

22 <sup>4</sup> Pew Research Internet Project, “Privacy and Data Management on Mobile Devices,” (Sept. 5,  
23 2012) <http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/>.

24 <sup>5</sup> Pew Research Internet Project, “Location-Based Services” (Sept. 12, 2013)  
<http://www.pewinternet.org/2013/09/12/location-based-services/>.

25 <sup>6</sup> Truste, “TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than  
26 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/>.

27 <sup>7</sup> Janice Y. Tsai, *et al.* “Location-Sharing Technologies: Privacy Risks and Controls,” Carnegie  
28 Mellon University, 12 (Feb. 2010) [http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh\\_2009.pdf](http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf).

1 and religious beliefs, sexual habits, and so on.” *Id.* at 956 (Sotomayor, J., concurring). And Justice  
2 Alito wrote “society’s expectation has been that law enforcement agents and others would not . . .  
3 secretly monitor and catalogue every single movement of an individual’s car for a very long  
4 period.” *Id.* at 964 (Alito, J., concurring).

5 Last month, in *Riley v. California*, the Supreme Court specifically cited Justice  
6 Sotomayor’s concurring opinion in *Jones* as a reason to limit police searches of cell phones  
7 incident to arrest. *Riley* recognized that cell phones store “qualitatively different” types of data  
8 compared to physical records, including data that can “reveal where a person has been,” making it  
9 possible to “reconstruct someone’s specific movements down to the minute, not only around town  
10 but also within a particular building.” *Riley*, 134 S. Ct. at 2490 (citing *Jones*, 132 S. Ct. at 955  
11 (Sotomayor, J., concurring)). *Riley* noted that because of data like this, the “scope of the privacy  
12 interests at stake” far exceeds that of anything in the physical world. *Id.* at 2491.

13 In the wake of *Jones*, several state and federal courts have also recognized the privacy  
14 implications of historical cell site data specifically. In protecting cell site data in *Commonwealth v.*  
15 *Augustine*, the Massachusetts Supreme Judicial Court recognized that this data may raise even  
16 greater privacy concerns than GPS tracking devices placed on a car because cell site data can track  
17 “the user’s location far beyond the limitations of where a car can travel”—including into  
18 “constitutionally protected areas” like a home. 4 N.E. 3d 846, 861-62 (Mass. 2014). *Augustine* also  
19 noted historical cell site data gave police access to something it would never have with traditional  
20 law enforcement investigative methods: the ability “to track and reconstruct a person’s past  
21 movements.” *Id.* at 865. In *State v. Earls*, the New Jersey Supreme Court adopted a warrant  
22 requirement for historical cell site data, holding users should be “entitled to expect confidentiality  
23 in the ever-increasing level of detail that cell phones can reveal about their lives.” 70 A.3d 630, 644  
24 (N.J. 2013). Most recently, in *United States v. Davis*, the Eleventh Circuit noted that one may  
25 assume that location information that could be revealed by even one point of cell site data—such as  
26 a person’s “first visit to a gynecologist, a psychiatrist, a bookie, or a priest”—is “private if it was  
27 not conducted in a public way.” --- F.3d ---, 2014 WL 2599917, \*8 (11th Cir. 2014).

1 While a person may take affirmative steps to broadcast her movements publicly—for  
2 example, by “checking in” or sharing her location over social media like Twitter or Facebook—  
3 historical cell site information is not “public” in this way. Instead, historical cell site information is  
4 private information disclosed to no one other than the phone company. *See Augustine*, 4 N.E.3d at  
5 862-63. As explained below, just because technology is *capable* of disclosing what is otherwise  
6 private information about a person’s specific location does not mean that a person has a lesser  
7 expectation of privacy under the Fourth Amendment.

8 **II. THE “THIRD-PARTY DOCTRINE” DOES NOT CHANGE THE EXPECTATION**  
9 **OF PRIVACY IN HISTORICAL CELL SITE INFORMATION.**

10 The government relies on *Smith v. Maryland* to argue cell phone users have no expectation  
11 of privacy in historical cell site records because that data has been exposed to a third party—the  
12 phone company. *See* Government’s June 26, 2014 Letter Brief at p. 4 (citing *Smith*, 442 U.S. at  
13 742-44). According to the government, when a person voluntarily uses a cell phone to make a call  
14 or respond to a text message, she knows the phone is sending information about her location to the  
15 cell phone company and thus cannot expect the phone company to keep that information private  
16 under *Smith*. But *Smith* does not alter the calculus here for two reasons.

17 First, cell phones present privacy issues vastly different from the technology at issue in  
18 *Smith*. The Supreme Court recently recognized this in *Riley*. In 1973, the Supreme Court in *United*  
19 *States v. Robinson* held police could search physical items—specifically a pack of cigarettes—  
20 found on an arrestee without a warrant incident to arrest. 414 U.S. 218, 236 (1973). But *Riley*  
21 refused to equate the cigarettes in *Robinson* with a modern cell phone, believing that comparing the  
22 two was “like saying a ride on horseback is materially indistinguishable from a flight to the moon.  
23 Both are ways of getting from point A to point B, but little else justifies lumping them together.”  
24 *Riley*, 134 S. Ct. at 2488. Instead, because modern cell phones implicate privacy concerns far  
25 beyond physical analogues addressed in past cases, any extension of reasoning from those past  
26 cases “to digital data has to rest on its own bottom.” *Id.* at 2489.

1 Similarly, here, because the data generated by cell site information is so different in  
2 quantity and quality from the data generated by a simple landline phone, this Court cannot rely  
3 only on antiquated cases in determining how to protect data on and generated by cell phones. 134  
4 S. Ct. at 2488-89. Instead, this Court should look to actual societal understandings of privacy in  
5 cell phone data and location information to determine the protections necessary to place on this  
6 information to satisfy the Fourth Amendment.

7 Second, *Smith* not only fails to capture the technology at issue here, it has also been rejected  
8 by the California Supreme Court. Just months after *Smith* was decided, the state high court ruled in  
9 *People v. Blair* that Californians have an expectation of privacy in their phone records under  
10 Article I, Section 13 of the state constitution, the state equivalent to the Fourth Amendment. 25  
11 Cal. 3d 640, 655 (Cal. 1979).<sup>8</sup> While *Smith* held phone customers have no subjective expectation of  
12 privacy in dialed phone numbers because they “convey” the numbers to the company to have the  
13 calls connected, 442 U.S. at 742, *Blair* instead focused on the fact that a list of telephone calls  
14 provides a “virtual current biography” of a person. 25 Cal. 3d at 653. Since it was “virtually  
15 impossible for an individual” to “function in the modern economy without a telephone,” these  
16 records were not voluntarily disclosed. *Id.* Thus, police need a warrant to obtain the records under  
17 the state constitution. *Id.* at 655; *see also People v. Chapman*, 36 Cal. 3d 98, 106-111 (1984),  
18 disapproved on other grounds in *People v. Palmer*, 24 Cal. 4th 856 (2001) (expectation of privacy  
19 in unlisted telephone number); *People v. McKunes*, 51 Cal. App. 3d 487, 492 (1975) (expectation  
20 of privacy in telephone company’s customer records).<sup>9</sup>

21 <sup>8</sup> Article 1, section 13 of the California constitution states in whole “The right of the people to be  
22 secure in their persons, houses, papers, and effects against unreasonable seizures and searches may  
23 not be violated; and a warrant may not issue except on probable cause, supported by oath or  
affirmation, particularly describing the place to be searched and the persons and things to be  
seized.”

24 <sup>9</sup> The California Attorney General has issued two opinions making clear that state law enforcement  
25 personnel must obtain a search warrant to install and use a pen register. First, in 1986, the Attorney  
26 General clarified that although California has no statutes governing pen registers, state magistrates  
27 were authorized to issue a search warrant supported by probable cause to permit police to install  
28 and use them. *See* 69 Ops. Cal. Atty. Gen 55 (1986). Later that year, Congress passed a set of  
federal statutes governing the installation and use of pen registers. *See* 18 U.S.C. §§ 3122-3127.  
Congress required state and federal law enforcement to obtain judicial authorization to install and

1 For this reason, the government’s argument that cell phone users within this Court’s  
2 jurisdiction in Northern California cannot expect location information to remain private once the  
3 data has been exposed to the phone company is incorrect. On the contrary, all Californians have  
4 been promised that third-party records generated by mundane but necessary acts, which reveal  
5 detailed biographical information about a person, are considered private.<sup>10</sup> That is precisely what  
6 historical cell site data is. Like bank records and dialed phone numbers, historical cell site  
7 information is capable of providing a “virtual current biography” of where a person has been, with  
8 whom they associate and their habits and patterns of movements. And, like these records,  
9 disclosing cell site records to a cell phone provider is not a truly voluntary act because it is virtually  
10 impossible to participate in contemporary society without generating them. *See Burrows*, 13 Cal.  
11 3d at 247 (bank records protected by state constitution even though they are shared with a third  
12 party because it is “impossible to participate in the economic life of contemporary society without  
13 maintaining a bank account.”).

14 Ultimately, that means this Court must reexamine the entire premise that *Smith* could be  
15 broad enough to encompass historical cell site records. At a minimum, the government cannot  
16 claim Californians have no subjective expectation of privacy in information the state has already  
17 promised its citizens is private, as finding no subjective expectation of privacy in these phone  
18 records would render state constitutional protection and *Blair*’s rejection of *Smith* meaningless.

---

19 use a pen register but only required the government to demonstrate the evidence obtained via pen  
20 register is “relevant to an ongoing criminal investigation” rather than require probable cause. 18  
21 U.S.C. §§ 3122(a)(2), (b)(2). For state law enforcement, the use of the federal pen register statute  
22 has to be consistent with state law. 18 U.S.C. § 3122(a)(2). So in 2003, the state Attorney General  
23 clarified that since *Blair* placed the information obtained from a pen register—a list of phone  
24 numbers dialed—within the “zone of privacy protected by the state Constitution,” state law  
25 enforcement could not rely on federal law to install a pen register. 86 Ops. Cal. Atty. Gen. 198 at  
26 \*3-4 (2003).

27 <sup>10</sup> The California Supreme Court has rejected the third-party doctrine in other contexts as well. For  
28 example, in *Burrows v. Super. Ct.*, the court held that California bank customers have an  
expectation of privacy in their bank records under the state constitution. 13 Cal. 3d 238, 247  
(1974). Since a bank customer “reveals many aspects of his personal affairs, opinions, habits and  
associations” when dealing with a bank, the records are protected. *Id.* That conclusion is at odds  
with the U.S. Supreme Court’s decision in *United States v. Miller*, 425 U.S. 435 (1976), which  
found no expectation of privacy in bank records.

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

5           Having established that advances in technology require changes in legal analyses, that  
6           people generally have a subjective expectation of privacy in their location, and that Californians  
7           specifically have an expectation of privacy in phone records and data capable of revealing a  
8           “virtual current biography” about a person, the question remains whether broader society is  
9           prepared to recognize that subjective expectation of privacy as reasonable. The answer is yes.

10           Immediately after *Smith* was decided, courts in eight states—including Colorado, Florida,  
11           Hawaii, Idaho, Illinois, New Jersey, Pennsylvania and Washington—followed California’s lead  
12           and rejected *Smith*, instead finding those states’ residents had a reasonable expectation of privacy  
13           under the state constitution in dialed phone numbers—notwithstanding the fact those records are  
14           held by the phone provider.<sup>11</sup> By statute, Georgia and Oregon required police to demonstrate  
15           probable cause to install and operate a pen register to obtain dialed phone numbers.<sup>12</sup>

16           Then, as technology continued to advance but before *Jones* was decided, the state supreme  
17           courts of New York, Oregon, and Washington held that people could reasonably expect privacy in  
18           their location, meaning that using technology to track a person’s movements was a Fourth  
19           Amendment “search.”<sup>13</sup> Five state legislatures passed statutes requiring police to obtain a probable  
20           cause search warrant to track a person’s location with a tracking device like a GPS—even when the  
21           person is traveling in public places.<sup>14</sup> This meant that even before the Supreme Court addressed the

22           

---

<sup>11</sup> See *People v. Sporleder*, 666 P.2d 135, 141-43 (Colo. 1983); *Shaktman v. State*, 553 So.2d 148,  
23           150-51 (Fla. 1989); *State v. Rothman*, 779 P.2d 1, 7-8 (Haw. 1989); *State v. Thompson*, 760 P.2d  
24           1162, 1165-67 (Id. 1988); *People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill.Ct.App. 1993); *State v.*  
25           *Hunt*, 450 A.2d 952, 955-57 (N.J. 1982); *Commonwealth v. Melilli*, 555 A.2d 1254, 1256-59 (Pa.  
26           1989); *State v. Gunwall*, 720 P.2d 808, 813-17 (Wash. 1986); see generally Stephen E. Henderson,  
27           *Learning From all Fifty States: How to Apply the Fourth Amendment and its State Analogs to*  
28           *Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

<sup>12</sup> 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.

<sup>13</sup> 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).

<sup>14</sup> See Haw. Rev. Stat. § 803-44.7(b); Okla. Stat. Ann. tit. 13, § 177.6(A); Or. Rev. Stat. Ann. §



1 question of whether Americans have a reasonable expectation of privacy in their location  
2 information, seven states, representing nearly 20% of the United States population<sup>15</sup> already  
3 recognized this privacy right.

4 After *Jones*, the number of people across the country reasonably expecting privacy in their  
5 location has increased, as more courts have recognized that an expectation of privacy in a person's  
6 location means technologies like GPS or real time cell phone tracking is a Fourth Amendment  
7 "search" under *Katz*.<sup>16</sup> *Jones* encouraged states to go further than they had before, particularly  
8 because Justice Sotomayor specifically questioned *Smith*, noting its "premise" was "ill suited to the  
9 digital age, in which people reveal a great deal of information about themselves to third parties in  
10 the course of carrying out mundane tasks." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).  
11 Honing in on subjective expectations of privacy, she doubted "people would accept without  
12 complaint the warrantless disclosure" of information to the government like URLs they visit or the  
13 phone numbers they dial or text. *Id.*

14 As explained above, that has extended to historical cell site data, with the high courts of  
15 Massachusetts and New Jersey—relying in part on Justice Sotomayor's concurrence—recognizing  
16 a reasonable expectation of privacy in historical cell site data under their respective state  
17 constitutions and requiring police to use a search warrant to obtain that information. Five more  
18 states legislated privacy protections for historical cell site data, with Colorado, Maine, Minnesota,  
19 Montana and Utah passing statutes expressly requiring law enforcement to apply for a search  
20 warrant to obtain this data.<sup>17</sup> And more courts reached the same conclusions as Justice Sotomayor

---

21 133.619(6); 18 Pa. Cons. Stat. Ann. § 5761(c)(4); S.C. Code Ann. § 17-30-140(b)(2).

22 <sup>15</sup> This figure is based on 2013 population data for each state, as projected by the U.S. Census. See  
23 United States Census Bureau, "Quick Facts," <http://quickfacts.census.gov/qfd/index.html>.

24 <sup>16</sup> *Commonwealth v. Rousseau*, 990 N.E.2d 543, 552-53 (Mass. 2013) (GPS); *Commonwealth v.*  
25 *Rushing*, 71 A.3d 939, 961-64 (Pa. Sup. Ct. 2013), *appeal granted on other grounds* 84 A.3d 699  
26 (2014) (cell phone signal); *State v. Brereton*, 826 N.W.2d 369, 379 (Wis. 2013) (GPS); *United*  
27 *States v. Powell*, 943 F. Supp. 2d 759, 776-77 (E.D. Mich. 2013) (real time cell site tracking); *State*  
28 *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).

<sup>17</sup> 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) (effective August 1, 2014); 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

1 in *Jones*, noting “the rapid expansion in the quantity of third-party data generated through new  
2 technologies raises important questions about the continued viability of the third-party doctrine in  
3 the digital age.” *Augustine*, 4 N.E.3d at 863 n. 35; *see also State v. Walton*, 324 P.3d 876, 905  
4 (Haw. 2014) (expectation of privacy in GNC membership account information).

5 Last month, the Eleventh Circuit Court of Appeals became the first federal appeals court to  
6 find an expectation of privacy in historical cell site records, holding police need a probable cause  
7 warrant to obtain them. *See Davis*, 2014 WL 2599917, \*10.<sup>18</sup> Because *Davis* controls the actions of  
8 both federal and state law enforcement, people in Alabama, Florida and Georgia now have a  
9 reasonable expectation of privacy in historical cell site information. In sum, the number of people  
10 in the United States who have been promised by court decision or legislation that information  
11 about where they have been—either at a specific moment or over an extended period of time—has  
12 never been higher. While not dispositive of whether there is a Fourth Amendment expectation of  
13 privacy in historical cell site data, the growing number of people protected by the warrant  
14 requirement is compelling proof of “societal understandings” as to what level of privacy and  
15 security is reasonable.

16 Although the Eleventh Circuit’s decision in *Davis* parts ways with the Fifth Circuit’s  
17 decision in *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013),  
18 which found no expectation of privacy in historical cell site data, this Court writes on a blank slate.  
19 The Ninth Circuit has already suggested that *Smith* does not necessarily control all situations  
20 involving technology that captures information controlled by third parties. In *United States v.*  
21 *Forrester* the Court relied on *Smith* to find that the use of a pen register to capture IP address and  
22 other Internet metadata was not a Fourth Amendment “search.” 512 F.3d 500, 509-11 (9th Cir.  
23

24  
25 search warrant only to track a cell phone in real time. *See, e.g., Ind. Code 35-33-5-12; Wisc. Stat.*  
26 *Ann. § 968.373(2).*

27 <sup>18</sup> The Third Circuit Court of Appeals ruled in 2010 that a magistrate may, but is not required, to  
28 request the government apply for a search warrant to obtain historical cell site records. *In re*  
*Application of U.S. for an Order Directing a Provider of Electronic Communication Service to*  
*Disclose Records*, 620 F.3d 304, 319 (3d Cir. 2010).

1 2007). However, the court made clear it was not implying “more intrusive techniques or techniques  
2 that reveal more content-rich information” would lead to the same result. *Id.* at 511.

3 The opinions in *Davis*, *Augustine* and *Earls* and the state statutes requiring police obtain a  
4 warrant to get historical cell site records make clear that this location information is the more  
5 revealing and intrusive technique hinted at by *Forrester*. Coupled with the rejection of *Smith* in  
6 California law and the growing number of people for whom historical cell site data is protected by  
7 a warrant requirement, this shows the government must use a search warrant to obtain historical  
8 cell site data.

### 9 CONCLUSION

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

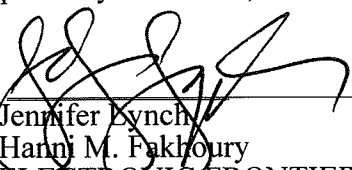
16 When it comes to historical cell site records, it is clear that Americans generally and  
17 Californians specifically expect that the location information revealed by these records remain  
18 private. Given the growing trend in legislatures and courts across the country to protect this privacy 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

20 This court should follow the Supreme Court’s lead in *Riley v. California* and recognize that,  
21 given the vast amount of data generated by cell phones, coupled with the trend toward greater  
22 privacy protections for that data, outdated cases cannot govern the outcome here. Americans have a  
23 reasonable expectation of privacy in the location data generated by cell site location information,  
24 and, as the Court noted in *Riley*, the answer to the question of what police must do before they may  
25 obtain that data “is simple—get a warrant.” 134 S. Ct. at 2495.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DATED: July 29, 2014

Respectfully submitted,

By: 

Jennifer Lynch  
Hanni M. Fakhoury  
ELECTRONIC FRONTIER FOUNDATION  
815 Eddy Street  
San Francisco, CA 94109  
Telephone: (415) 436-9333  
Facsimile: (415) 436-9993

Counsel for *Amicus Curiae*  
ELECTRONIC FRONTIER FOUNDATION

1 CERTIFICATE OF SERVICE

2 I HEREBY CERTIFY that on July 29, 2014, I filed the foregoing with the Clerk of the  
3 Court and caused to be served by U.S. Mail, postage thereon fully prepaid, a true and correct copy  
4 of the foregoing on:

5 Ellen Valentik Leonida  
6 Federal Public Defender's Office  
7 555 12th Street , Suite 650  
8 Oakland, CA 94607-3627  
9 (510) 637-3500  
10 Fax: (510) 637-3507  
11 Email: ellen\_leonida@fd.org

12 *Counsel for Defendant*

13 Damali A. Taylor  
14 U.S. Attorney's Office  
15 450 Golden Gate Avenue, Box 36055  
16 San Francisco, CA 94102  
17 415-436-6401  
18 Email: damali.taylor@usdoj.gov

19 *Counsel for Plaintiff*

20 I declare under penalty of perjury under the laws of the United States that the foregoing is  
21 true and correct. Dated this 29<sup>th</sup> day of July, 2014.

22   
23 \_\_\_\_\_  
24 Stephanie Shattuck