

1 MARCIA HOFMANN (Cal. Bar No. 250087)  
marcia@marciahofmann.com  
2 25 Taylor Street  
San Francisco, CA 94102  
3 Telephone: (415) 830-6664

4 *Attorney for Amicus Curiae*  
*Professor Susan Freiwald*

6 IN THE UNITED STATES DISTRICT COURT  
7 THE NORTHERN DISTRICT OF CALIFORNIA  
8 SAN FRANCISCO DIVISION

9 IN RE TELEPHONE INFORMATION )  
10 NEEDED FOR A CRIMINAL )  
11 INVESTIGATION )  
12 )  
13 )  
14 )  
15 )

) Case No. 3:14-XR-90532 NC  
)  
)  
) **BRIEF AMICUS CURIAE OF PROFESSOR**  
) **SUSAN FREIWALD IN OPPOSITION TO**  
) **THE GOVERNMENT'S SEALED**  
) **APPLICATIONS FOR CELL SITE**  
) **LOCATION INFORMATION**

16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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

**STATEMENT OF INTEREST**

*Amicus* is a law professor at the University of San Francisco School of Law who teaches and writes about cyber law and information privacy law. She has written several law review articles on how the Fourth Amendment and federal surveillance statutes should apply to new communications technologies, including *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004); *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011); and *Light In the Darkness: How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 875 (2014).

Professor Freiwald has submitted several *amicus* briefs in other cases addressing the Fourth Amendment’s application to emerging electronic surveillance techniques, including in the Sixth Circuit concerning the Fourth Amendment protection of stored email and in the Third and Fifth Circuits addressing the Fourth Amendment protection of location data. She has no stake in the outcome of this case, but is committed to ensuring that the law evolves to protect the vital role electronic communications play in our lives.

**SUMMARY OF ARGUMENT**

Cell site location information can expose a great deal about someone’s life. When the government acquires information about a person’s location, it intrudes on that person’s reasonable expectation of privacy. This Court should find that the compelled disclosure of historical cell site location information is a Fourth Amendment search that requires a probable cause warrant. This approach follows the lead of the Supreme Court and appeals courts, which have recognized that searches of digital information present unique considerations, and the judiciary should serve as a check on those searches to protect individual privacy. Rather than accepting the government’s attempt to stretch archaic precedents past their breaking points, this Court should deny the sealed applications and simply tell the government, in the words of Chief Justice Roberts, to “get a warrant.” *Riley v. California*, 134 S. Ct. 2473, 2494 (2014).

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

**ARGUMENT**

**I. COMPELLED DISCLOSURE OF HISTORICAL CELL SITE LOCATION INFORMATION IS A FOURTH AMENDMENT SEARCH THAT REQUIRES A PROBABLE CAUSE WARRANT.**

Cell site location information (“CSLI”) has the potential to reveal intimate details about a person’s day-to-day life. Location data shows patterns of movement and behavior that may expose health conditions, political beliefs, religious affiliations, and intimate relationships. When the government compels service providers to disclose CSLI, it engages in an intrusive surveillance method with a high risk of abuse. Because this practice encroaches on our reasonable expectations of privacy in how we conduct our everyday activities, the courts increasingly recognize that the acquisition of historical location data by the government is a Fourth Amendment search that requires a neutral magistrate to issue a warrant based on a finding of probable cause.<sup>1</sup> The Court should follow suit and deny the government’s sealed applications for cell site location information.

**A. The Eleventh Circuit Properly Applied the Fourth Amendment in *United States v. Davis* to Conclude That Individuals Have Reasonable Expectations of Privacy in Historical Cell Site Location Information.**

Last month, the Eleventh Circuit concluded in *United States v. Davis* that the government violates the Fourth Amendment when it compels providers to disclose even a single point of stored location data without first obtaining a warrant based on probable cause. \_\_ F.3d \_\_, No. 12-12928, 2014 WL 2599917, at \*8 (11th Cir. June 11, 2014).

*Davis* is particularly persuasive because of its comprehensive and rigorous analysis. The unanimous opinion reflects nuanced consideration of the sensitivity of location data and its vast implications for Fourth Amendment law, and also takes into account specifically the potential for law enforcement abuse of CSLI. *Id.* at \*\*4-9. *Davis* recognizes that what makes CSLI valuable to law enforcement—its ability to deliver incriminating detail about search targets’ location—

---

<sup>1</sup> See generally Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011).

1 increases the risk that the government will invade those targets' privacy more broadly: "While  
2 committing a crime is certainly not within a legitimate expectation of privacy, if the cell site  
3 location data could place him near those scenes, it could place him near any other scene. There is a  
4 reasonable privacy interest in being near the home of a lover, or a dispensary of medication, or a  
5 place of worship, or a house of ill repute." *Id.* at \*9.

6 Importantly, *Davis* incorporates and relies upon the Supreme Court's finding of a Fourth  
7 Amendment interest in location privacy in *United States v. Jones*, 132 S. Ct. 945 (2012). This  
8 makes the Eleventh Circuit's approach more instructive than the Third Circuit's, which predated  
9 *Jones* and did not benefit from the Supreme Court's direction. *In re Application of the U.S. for an*  
10 *Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't (Third*  
11 *Circuit Decision)*, 620 F.3d 304 (3d Cir. 2010).<sup>2</sup>

12 The *Davis* court followed the Supreme Court's lead when it applied the reasonable  
13 expectation of privacy test to the government's acquisition of location data. The Eleventh Circuit  
14 noted that *Jones* clearly retained the test from *Katz v. United States*, 389 U.S. 347, 361 (1967)  
15 (Harlan, J., concurring), to determine whether an investigative method constitutes a search that  
16 implicates the Fourth Amendment. *Davis*, 2014 WL 2599917, at \*8. While *Jones* ultimately relied  
17 on the trespassory installation of a GPS device to find that a Fourth Amendment search had  
18 occurred, the Court emphasized that "[s]ituations involving merely the transmission of electronic  
19 signals without trespass would *remain* subject to [the] *Katz* [privacy] analysis." *Jones*, 132 S. Ct.  
20 at 953 (emphasis in original).

21 While the *Jones* majority and concurring opinions focused on the potential for aggregated  
22 location data to be especially intrusive, *Davis* held that even a lone point of cell site location data  
23 could fall within a reasonable expectation of privacy. *Davis*, 2014 WL 2599917, at \*8. A person  
24 can carry her cell phone with her anywhere in her purse or pocket, enabling her movements to be  
25 tracked over time. Regardless, she is entitled to assume that even her "first visit to gynecologist, a  
26

27 <sup>2</sup> Further, the Third Circuit defused the Fourth Amendment question by finding that magistrate  
28 judges have the discretion under the Stored Communications Act to require the government to  
secure a warrant based on probable cause to obtain CSLI. 620 F.3d at 319.

1 psychiatrist, a bookie, or a priest . . . is private if it was not conducted in a public way.” *Id.* Thus,  
2 the Eleventh Circuit said that cell site data should *always* be considered private, not only in  
3 situations where investigators have collected a “sufficient mosaic to expose that which would  
4 otherwise be private.” *Id.* By finding Fourth Amendment protection in CSLI regardless of the  
5 amount of information collected, *Davis* presents a workable bright-line test that other courts can  
6 easily apply.<sup>3</sup>

7 The *Davis* rule is a logical extension of the seminal test in *Katz*. The Supreme Court found  
8 that *Katz* was entitled to believe his conversation inside a phone booth on a public street was  
9 private, regardless of how much or little the government could overhear with the aid of an  
10 electronic device. 389 U.S. at 352. Likewise, the *Davis* court found that people are entitled to  
11 believe that their daily movements from one place to another are within their expectations of  
12 privacy so long as those movements “are not conducted in a public way.” *Davis*, 2014 WL  
13 2599917, \*8.

14  
15 **B. The Supreme Court’s Recent Decision in *Riley v. California* Aligns with the  
16 *Davis* Approach.**

17 The Supreme Court’s decision last month in *Riley v. California* buttressed the Eleventh’s  
18 Circuit’s reasoning in *Davis*. 134 S. Ct. 2473. The *Riley* Court determined that Fourth Amendment  
19 reasonableness generally requires a warrant for searches of cell phones incident to arrest,  
20 notwithstanding that agents may search the physical effects immediately associated with an  
21 arrestee’s person without obtaining a warrant. *Id.* at 2481-82, 2484-85. The Court explained that  
22 this distinction was appropriate because of the unique nature of the cell phone and the vast  
23 information commonly stored on it. *Id.* at 2485, 2489-91.

24 *Riley*’s categorical refusal to extend the search-incident-to-arrest exception to cell phone  
25 searches parallels *Davis*’ holding that acquisition of any cell site location data requires a warrant.

26  
27 <sup>3</sup> An influential legal scholar has criticized the “mosaic theory” for being unworkable in practice.  
28 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 328-43  
(2012); see also Freiwald, *supra* note 1, at 748-49 (contending that all acquisitions of historical  
CSLI are Fourth Amendment searches).

1 The Supreme Court chose not to adopt a more fact-specific, case-by-case approach to permit the  
2 exception under some circumstances.<sup>4</sup> *Riley*, 134 S. Ct. at 2491-92. Instead, the Supreme Court  
3 gave clear guidance to law enforcement agents and lower courts to constrain law enforcement  
4 discretion. *Id.* at 2491-93.

5 *Riley*'s preference for a workable rule affirms the wisdom of *Davis* over the single other  
6 post-*Jones* appellate decision on CSLI, *In re Application of U.S. for Historical Cell Site Data*  
7 (*Fifth Circuit Decision*), 724 F.3d 600 (5th Cir. 2013).<sup>5</sup> Rather than treating all historical location  
8 records as a single category of information that should be protected by the Fourth Amendment, the  
9 Fifth Circuit allowed the government to obtain a small subset of location information—the points  
10 at which the user places and terminates a call—without a warrant. *Id.* at 615. The court explicitly  
11 declined to address the constitutionality of orders seeking anything more. *Id.* Thus, the Fifth  
12 Circuit's narrow, fact-specific decision fails to offer magistrate judges much guidance about how  
13 to address the great bulk of current and pending location data requests.<sup>6</sup>

14 While *Riley* addressed the search of a cell phone's contents rather than the compelled  
15 disclosure of records from a provider, its factual findings and method of analysis directly pertain  
16 to this case. The Court recognized that modern cell phones are sophisticated computers that serve  
17 as "cameras, video players, rolodexes, calendars, tape records, libraries, diaries, albums,  
18 televisions, maps, or newspapers." *Riley*, 134 S. Ct. at 2489. A cell phone's useful multi-  
19 functionality no doubt explains why most people keep these devices with them around the clock.  
20 *Id.* at 2490 (citing poll that found nearly three-quarters of smart phone users reported spending  
21 most of their time within five feet of their phones). The central role that cell phones play in our

---

22 <sup>4</sup> The Court did, however, emphasize that the exigent circumstances exception to the warrant  
23 requirement continues to be a viable fact-specific exception to the warrant requirement. *Riley*, 134  
24 S. Ct. at 2486, 2494.

25 <sup>5</sup> Two recent state Supreme Courts have required a warrant under their state constitutions for the  
26 compelled disclosure of historical location data. See the Electronic Frontier Foundation's *amicus*  
27 brief discussing *Commonwealth v. Augustine*, 467 Mass. 230 (Mass. 2014) and *State v. Earls*, 70  
28 A.3d 630 (N.J. 2013).

<sup>6</sup> See Susan Freiwald, *Light In the Darkness: How the LEATPR Standards Guide Legislators in  
Regulating Law Enforcement Access to Cite Site Location Records*, 66 OKLA. L. REV. 875, 892-93  
(2014).

1 lives means that law enforcement can use historical location data from a device to “reconstruct  
2 someone’s specific movements down to the minute, not only around town but also within a  
3 particular building.” *Id.*

4 When new technologies like cell phones raise heightened privacy concerns, courts should  
5 not mechanically apply historical precedents developed in very different contexts. *Riley*, 134 S. Ct.  
6 at 2484-85 (majority); 2496 (Alito, J., concurring). The Supreme Court refused to treat searches of  
7 cell phones like searches of physical objects because “that would be like saying a ride on  
8 horseback is materially indistinguishable from a flight to the moon.” *Id.* at 2488. Likewise, *Davis*  
9 found a reasonable expectation of privacy in public movements despite outdated precedent that  
10 declined to do so. *Compare Davis*, 2014 WL 2599917, at \*8, and *United States v. Knotts*, 460 U.S.  
11 276, 281-82 (1983) (finding no expectation of privacy in a vehicle’s movements along public  
12 highways, tracked by a radio beeper). This Court should follow suit and find a reasonable  
13 expectation of privacy in CSLI.

14 **II. THE ANTIQUATED THIRD-PARTY DOCTRINE SHOULD NOT BE STRETCHED TO ALLOW**  
15 **THE ACQUISITION OF HISTORICAL CELL SITE DATA WITHOUT A WARRANT.**

16 *Riley* made clear that cell phones require “a new balancing of law enforcement and privacy  
17 interests” rather than a reflexive application of old rules to new technology. *Riley*, 134 S. Ct. at  
18 2496-97 (Alito, J., concurring), 2484-85 (majority). And yet the government relies on *United*  
19 *States v. Miller*, 425 U.S. 443 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), to argue that  
20 people lack reasonable expectations of privacy in historical cell site information. Gov. June 26,  
21 2014 Letter Brief at 2-6. Over thirty years ago these cases established the “third-party doctrine,”  
22 which maintains that a person has no reasonable expectation of privacy in information voluntarily  
23 disclosed to a third party. But more recent precedent from the Supreme Court and appellate courts  
24 disfavors the third-party rule’s application to digital information disclosed to service providers.  
25 *See, e.g., Jones*, 123 S. Ct. at 957 (Sotomayor, J., concurring) (the third-party rule is “ill suited to  
26 the digital age, in which people reveal a great deal of information about themselves to third parties  
27 in the course of carrying out mundane tasks.”).

1 Using *Smith* and *Miller* as a foundation, the government argues that the Fourth  
2 Amendment should not extend to CLSI because users voluntarily transmit signals to cell phone  
3 towers just as they transmit phone numbers. Gov. June 26, 2014 Letter Brief at 3-4. The  
4 government also claims that it can obtain historical cell site records by labeling them business  
5 records and choosing to obtain an order under 18 U.S.C. § 2703(d). Gov. June 26, 2014 Letter  
6 Brief at 5.

7 These arguments ignore the fact that CSLI can become a meticulous portrait of a person's  
8 location over time. As cell phone towers become smaller and more pervasive, their proximity to  
9 targets becomes closer and the information about location they provide more precise. *The*  
10 *Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance:*  
11 *Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H.*  
12 *Comm. on the Judiciary*, 113th Cong. 11-12 (2013) (testimony of Matt Blaze, Associate Professor,  
13 University of Pennsylvania);<sup>7</sup> *Riley*, 134 S. Ct. at 2490. Indeed, under some circumstances, cell  
14 site data can be precise enough to pinpoint a cell phone's location inside rooms or on particular  
15 floors of a building. *Id.*

16 This information could be used to construct a granular profile of a person's movements  
17 and associations day in and day out, even reaching into spaces that are highly protected under the  
18 Fourth Amendment, such as homes and other sensitive spaces. *See Riley*, 134 S. Ct. at 2490  
19 (describing how location monitoring “reflects a wealth of detail about [a person's] familial,  
20 political, professional, religious, and sexual associations.”) (quoting *Jones*, 123 S. Ct. at 955  
21 (Sotomayor, concurring)). In *Davis*, the CSLI evidence was so precise “that the prosecutor  
22 expressly relied on it in summing up to the jury in arguing the strength of the government's case  
23 for Davis's presence at the crime scenes.” 2014 WL 2599917, at \*3.

24 The Supreme Court signaled in *Riley* that it recognizes the implications of the  
25 government's argument and would likely reject it. The Court noted that a cell phone could be used  
26 to access information residing on a service provider's computer servers rather than stored locally  
27

28 <sup>7</sup> Available at [http://www.crypto.com/papers/blaze-20130425\\_final.pdf](http://www.crypto.com/papers/blaze-20130425_final.pdf).

1 on the cell phone itself. 134 S. Ct. at 2491. The Court could have applied *Smith* and *Miller* to find  
2 that the Fourth Amendment does not extend to a search of remotely stored information because  
3 that data has been voluntarily conveyed to the provider, or constitutes a business record of the  
4 provider. But instead the Court said, “Such a search would be like finding a key in a suspect’s  
5 pocket and arguing that it allowed law enforcement to unlock and search a house.” *Id.* *Davis*  
6 similarly found that we do not forfeit our reasonable expectations of privacy in our CSLI just  
7 because that information is conveyed to telecommunications carriers. 2014 WL 2599917, at \*10.  
8 Thus, people can have a reasonable expectation of privacy in information they disclose to a third-  
9 party provider.

10 *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) presents a more sensible rule for  
11 modern location data acquisition than *Smith* and *Miller*.<sup>8</sup> In *Warshak*, the Sixth Circuit held that a  
12 person has a reasonable expectation in the content of emails stored with a third-party service  
13 provider. *Id.* at 288. *Warshak* said that the service provider acts as an intermediary to transmit  
14 email, just like a phone company places phone calls or the post office delivers mail. *Id.* at 286-88.  
15 Thus, the use of an email service provider to deliver email does not extinguish a person’s  
16 expectation of privacy in her stored messages. *Id.* at 286.

17 Like the email provider in *Warshak*, a cell phone service provider is an intermediary that  
18 transmits its subscribers’ communications. And under *Davis*, the Fourth Amendment “covers not  
19 only [the] content [of communications], but also the transmission itself when it reveals  
20 information about the personal source of the transmission, specifically his location.” *Davis*, 2014  
21 WL 2599917, at \*5. Just as storage by email intermediaries does not nullify users’ expectations of  
22 privacy in their stored emails, cell phone users maintain reasonable expectations of privacy in the  
23 location data stored by their provider intermediaries. *Id.* at \*8 (“[C]ell site data is more like  
24 communications data than it is like GPS information.”)

25  
26  
27 <sup>8</sup> The Third Circuit also rejected application of the third-party rule. *Third Circuit Decision*, 620  
28 F.3d at 317-18; *see also* Freiwald, *supra* note 6, at 898-903 (discussing the Third Circuit’s  
analysis).

1 **III. IF THE COURT DETERMINES THE GOVERNMENT MAY OBTAIN HISTORICAL CELL SITE**  
2 **RECORDS WITHOUT A WARRANT, THE COURT SHOULD GUARD AGAINST OVERREACH.**

3 Should this Court disagree with *Davis* and decide that the government can obtain at least  
4 some CSLI without a warrant, the Court should examine the sealed applications carefully to  
5 ensure the government is not overreaching in its requests.

6 The government's publicly filed letter brief notes that law enforcement seeks historical cell  
7 site location information from AT&T and T-Mobile, and "as a general matter, cell phone providers  
8 compile cell site information from the beginning and end of a call." Gov. June 26, 2014 Letter  
9 Brief at 1, 4. The government presumably seeks these data points at a minimum. If the government  
10 seeks more information (such as location data about calls made to the target or about the person  
11 who made such calls), and to the extent it seeks cell tower information collected during calls or  
12 when the phone was idle, such information goes beyond what the Fifth Circuit permitted the  
13 government to obtain without a warrant. *Fifth Circuit Decision*, 724 F.3d at 615. Nor should the  
14 government be permitted to obtain any location information pertaining to text messages or access  
15 to the internet without a warrant.<sup>9</sup>

16 Finally, this Court should be wary about the possibility that the government may attempt to  
17 obtain real-time or prospective cell site information under the guise of historical records. If the  
18 government has requested that the provider disclose location records that have not yet been  
19 created, then it must obtain a warrant for a tracking device under Rule 41 of the Federal Rules of  
20 Criminal Procedure and may not proceed under Stored Communications Act provisions. *In re*  
21 *Application of the United States for an Order Authorizing Prospective and Continuous Release of*  
22 *Cell Site Location Records*, No. H:13-1198M, 2014 WL 3513120 (S.D. Tex. July 15, 2014).<sup>10</sup> See

23 <sup>9</sup> See, e.g., *In re Application of U.S. for an Order Authorizing Disclosure of Historical Cell Site*  
24 *Information for Telephone Number [Redacted]*, No. 14-286 (JMF), 2014 WL 1395082, at \*2  
(D.D.C. Apr. 17, 2014).

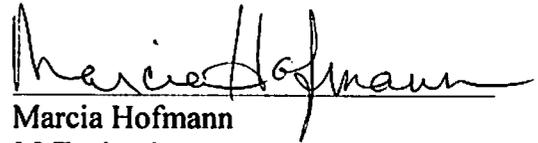
25 <sup>10</sup> The application in that case requested "For the target device, after receipt and storage, records or  
26 other information pertaining to the subscriber(s) or customers(s), including the means and source  
27 of payment for the service and cell site information provided to the United States on a continuous  
28 basis contemporaneous with (a) the origination of a call from the Target Device or the answer of a  
call to the Target Device, (b) the termination of the call and (c) if reasonably available, during the  
progress of the call, but not including the contents of the communication." 2014 WL 3513120, at  
\*1 n.1.

1 also *United States v. Espudo*, 954 F. Supp. 2d 1029, 1034-37, 1043 (S.D. Cal. 2013).

2  
3 **CONCLUSION**

4 For the foregoing reasons, *amicus* respectfully asks that the Court deny the government's  
5 sealed applications and require the government to seek a warrant based on probable cause to  
6 obtain CLSI.

7  
8  
9 Dated: July 29, 2014



Marcia Hofmann  
25 Taylor Street  
San Francisco, CA 94102  
Telephone: (415) 830-6664  
marcia@marciahofmann.com

*Attorney for Amicus Curiae*  
*Professor Susan Freiwald*

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

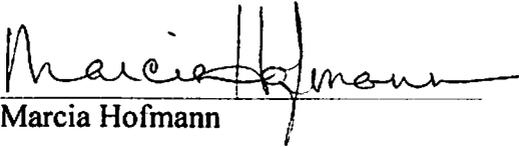
**CERTIFICATE OF SERVICE**

I certify that a true and correct copy of the foregoing Brief *Amicus Curiae* of Professor Susan Freiwald was sent via first class mail to the following on July 29, 2014:

Ellen Valentik Leonida  
Federal Public Defender's Office  
555 12th Street  
Suite 650  
Oakland, CA 94607-3627

J. Douglas Wilson  
Damali A. Taylor  
United States Attorney  
450 Golden Gate Avenue  
San Francisco, CA 94102

Dated: July 29, 2014

  
\_\_\_\_\_  
Marcia Hofmann