NO. 15-2443

UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

DAMIAN L. PATRICK,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the Eastern District of Wisconsin
Case No. 2:13-cr-00234-RTR-1
The Honorable Rudolph T. Randa, District Court Judge

MOTION OF ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AND ACLU OF WISCONSIN, INC. FOR LEAVE TO FILE AMICUS BRIEF IN SUPPORT OF DEFENDANT-APPELLANT

Adam Schwartz
Counsel of Record
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St.
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
adam@eff.org

Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Fl.
New York, NY 10004
Telephone: (212) 549-2500
Facsimile: (212) 549-2654
nwessler@aclu.org

Laurence J. Dupuis
ACLU OF WISCONSIN, INC.
207 E. Buffalo St., #325
Milwaukee, WI 53202
Telephone:
(414) 272-4032, ext. 212
ldupuis@aclu-wi.org

Attorneys for *Amici Curiae*

INTRODUCTION

Pursuant to Federal Rules of Appellate Procedure 27 and 29, the Electronic Frontier Foundation (EFF), the American Civil Liberties Union (ACLU) and ACLU of Wisconsin respectfully move this Court for leave to file an *amicus curiae* brief, in support of Defendant-Appellant Damian L. Patrick. Defendant-Appellant consents to the filing of this brief and Appellee United States has not taken a position one way or the other.

This Court has recognized that *amicus* briefing may be helpful in certain circumstances, such as "when the amicus has a unique perspective, or information, that can assist the court of appeals beyond what the parties are able to do." *Nat'l Org. for Women, Inc. v. Scheidler*, 223 F.3d 615, 617 (7th Cir. 2000). The Court may also consider (a) whether one of the parties "sponsored or encouraged" the filing of the *amicus* brief, and (b) whether the *amicus* brief "merely duplicates the brief of one of the parties." *Id.* All three of these factors weigh in favor of granting this motion and permitting the filing of the attached *amici curiae* brief.

STATEMENT OF INTEREST

EFF is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for 25 years. With roughly 26,000 active donors and dues-paying members nationwide, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age.

EFF has filed amicus briefs with this Court in numerous cases involving the application of constitutional principles to emerging technologies. *See, e.g., Belleau v.*

Wall, Case No. 15-3225 (7th Cir. 2015); *Backpage.com, LLC v. Dart*, 807 F.3d 229 (7th Cir. 2015); *McCarthy v. Langsenkamp Family Apostolate*, No. 15-1839 (7th Cir. 2015); *United States v. Daoud*, 755 F.3d 479 (7th Cir. 2014). EFF also has filed amicus briefs with the U.S. Supreme Court in cases addressing Fourth Amendment protections. *See, e.g., Riley v. California*, 134 S. Ct. 2473 (2014); *Maryland v. King*, 133 S. Ct. 1958 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012).

The ACLU is a nationwide, non-profit, non-partisan public interest organization of more than 500,000 members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU of Wisconsin is a state affiliate of the national ACLU, with 7,000 members around the state. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to both organizations. The ACLU and ACLU of Wisconsin have been at the forefront of numerous state and federal cases addressing the right of privacy and have served as counsel or amicus in numerous cases involving GPS and cell phone location tracking.

I. *Amici* are Not Affiliated With Any Party

No party or party's counsel has authored this brief in whole or in part. No party, party's counsel, or other person has contributed money that was intended to fund preparing or submitting the brief. Neither EFF, nor ACLU, nor ACLU of Wisconsin are sponsored by or in any way affiliated with any of the parties to this case. *Amici* file this brief to further their independent interests in protecting location privacy and preserving long-held Fourth Amendment liberties.

II. *Amici's* Brief Offers a Unique Perspective and Does Not Duplicate the Brief of One of the Parties

Finally, *Amici's* brief does not merely duplicate Appellant's brief. Rather, it provides the Court with a unique and important perspective on the broader implications of cellphone tracking, including information on the precision with which cellphones and cellphone service providers may capture data about where the phone's owner has travelled throughout their day, the privacy interests implicated by the government's collection of location data, the current trend toward greater legal protection for this data throughout the United States, and the implications of cellphone location data collection for Fourth Amendment analysis.

CONCLUSION

The brief of *amici curiae* EFF, ACLU and ACLU of Wisconsin meets the requirements of Federal Rule of Appellate Procedure 29 and provides the Court with an important perspective not offered by the parties to the litigation. For the reasons discussed above, *amici* respectfully request that this Court grant leave to file the accompanying brief.

Dated: January 22, 2016

By: /s/ Adam Schwartz

Adam Schwartz
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad St., 18th Fl.
New York, NY 10004

Laurence J. Dupuis
ACLU OF WISCONSIN, INC.
207 E. Buffalo St., #325
Milwaukee, WI 53202

Counsel for *Amici Curiae*

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 Seventh Circuit by using the appellate CM/ECF system on January 22, 2016.

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: January 22, 2016

By: */s/ Adam Schwartz*
Adam Schwartz
Counsel for Amici Curiae

NO. 15-2443

UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

DAMIAN L. PATRICK,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the Eastern District of Wisconsin
Case No. 2:13-cr-00234-RTR-1
The Honorable Rudolph T. Randa, District Court Judge

BRIEF *AMICI CURIAE* OF ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AND ACLU OF WISCONSIN, INC. IN SUPPORT OF DEFENDANT-APPELLANT

Adam Schwartz
Counsel of Record
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St.
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
adam@eff.org

Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Fl.
New York, NY 10004
Telephone: (212) 549-2500
Facsimile: (212) 549-2654
nwessler@aclu.org

Laurence J. Dupuis
ACLU OF WISCONSIN, INC.
207 E. Buffalo St., #325
Milwaukee, WI 53202
Telephone:
(414) 272-4032, ext. 212
ldupuis@aclu-wi.org

Attorneys for *Amici Curiae*

RULE 26.1 DISCLOSURE STATEMENT

Amici curiae Electronic Frontier Foundation, American Civil Liberties Union Foundation, and ACLU of Wisconsin, Inc. are non-profit public advocacy organizations. *Amici* have not appeared earlier in this case and no attorney from any other organization or law firm has appeared, or is expected to appear, on behalf of *amici curiae* in this case.

Amici state that they do not have a parent company, subsidiary or affiliate, and do not issue shares to the public.

Dated: January 22, 2016

By: /s/ Adam Schwartz

Adam Schwartz
ELECTRONIC FRONTIER FOUNDATION
Counsel of Record for *Amici Curiae* pursuant to Circuit Rule 3(d)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for 25 years. With roughly 26,000 active donors and dues-paying members nationwide, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age. EFF has filed *amicus* briefs with this Court in cases involving the application of constitutional principles to emerging technologies and has served as counsel or *amicus* in numerous state and federal cases involving the application of the Fourth Amendment to new technologies such as cell phone location information.

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan public interest organization of more than 500,000 members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU of Wisconsin is a state affiliate of the national ACLU, with 7,000 members around the state. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to both organizations. The ACLU and ACLU of Wisconsin have been at the forefront of numerous state and federal cases addressing the right of privacy, and have served as counsel or *amicus* in numerous cases involving GPS and cellphone location tracking.

---

[1] No party or party's counsel has authored this brief in whole or in part. No party, party's counsel, or other person has contributed money that was intended to fund preparing or submitting the brief. Appellant consents to the filing of this brief. Appellee has not taken a position one way or the other.

ARGUMENT

I. The Fourth Amendment Protects Location Privacy

Owning a cellphone is not a luxury; today more than 90% of all American adults have a cellphone,[2] and landline phones are becoming increasingly obsolete.[3] Cellphones generate a staggering amount of data about where the phone's owner has travelled throughout her daily life. This information about where we go exposes who we are. People take "indisputably private" trips, including "to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *United States v. Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring) (quoting *People v. Weaver*, 909 N.E.2d 1195, 11993 (N.Y. 2009)). These trips can reveal a great deal about a person. As the District of Columbia Circuit explained, "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd*, *Jones*, 132 S.Ct. 945.

---

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

[3] *See* Stephen J. Blumberg, Ph.D., & Julian V. Luke, *Wireless Substitution: Early Release of Estimates From the National Health Interview Survey, January–June 2015*, National Center for Health Statistics (Dec. 2015), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201512.pdf (noting that, as of June 2015, nearly one-half of American homes (47.4%) had only a cellphone, and that "more than two-thirds of all adults aged 25-34 and of adults renting their homes were living in wireless-only households").

"[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *See Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)) (Harlan, J., concurring)). Numerous opinion studies and advances in state law demonstrate both that Americans have a subjective expectation of privacy in their location information and that a growing portion of society recognizes this expectation as reasonable.

A. Cellphone Location Tracking Reveals Private and Increasingly Precise Information About Individuals' Locations and Movements

Because of capabilities built into cellphone networks and handsets in response to federal regulatory requirements, cellular service providers are able to precisely locate cellphones upon law enforcement requests. This capability stems from rules adopted in 1996 and implemented by 2001, under which the FCC required cellular service providers to have "the capability to identify the latitude and longitude of a mobile unit making a 911 call."[4] The precision and accuracy of this mandated cellphone location capability is increasing. In January 2015, the FCC adopted new rules to increase law enforcement's ability to identify the location of callers when they are indoors,[5] and require service providers to develop techniques

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

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

to determine the altitude of the phone, and thus which floor of a building it is located on.[6]

Although location capability was developed initially to assist in responding to 911 calls, service providers now provide the same location information to law enforcement pursuant to investigative requests. That is, law enforcement can ask a provider to generate new, precise, real-time location data by acquiring information from the target's phone. This can be done "on demand or at periodic intervals."[7] Some providers send periodic location updates via email, while Sprint, the provider at issue here, allows law enforcement "direct access to users' location data" by logging into an "automated . . . web interface." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc).[8]

The ability to locate and track a phone in real time has no relationship to whether the phone is in use. As long as the phone is on, law enforcement can request that the provider engage location tracking capabilities—a user cannot disable this functionality.[9] Even enabling location-privacy settings on the phone has

---

[6] Wireless E911 Order at 3-4.
[7] Matt Blaze, *How Law Enforcement Tracks Cellular Phones*, Exhaustive Search (Dec. 13, 2013) http://www.crypto.com/blog/celltapping/.
[8] *See also* Sprint, *Legal Compliance Guidebook* 7 (2008) https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_concordpd_concordnc.pdf at 568.
[9] *E.g. E911 Compliance FAQs*, Verizon Wireless, http://www.verizonwireless.com/support/e911-compliance-faqs/; *How Does E911 Work?*, Sprint, http://www.sprint.com/business/newsletters/articles/e911how_federal01.html.

no effect on the carrier's ability to determine the phone's precise location in real time: while these settings prevent third-party applications ("apps" like Google Maps) from accessing the phone's location information, they do not impact the carrier's ability to do the same.

Providers can obtain the location of a cellphone upon law enforcement request in at least two ways, depending on the structure of the carrier's network. The user's location can be determined by using hardware built into the phone ("handset-based" technology) and/or by analyzing the phone's interactions with the network's base stations, or "cell sites" ("network-based" technology).[10] Sprint uses handset-based technology.[11]

Handset-based technology uses a cellphone or other mobile device's "special hardware that receives signals from a constellation of GPS satellites."[12] The GPS chip installed in a cellphone uses radio signals from satellites orbiting the earth to calculate its own location within 10 meters.[13] Newer receivers with enhanced communication-to-ground-based technologies that correct signal errors can identify

---

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

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

[12] Blaze Hearing Statement at 7; Wireless E911 Order at 5 n.11.

[13] Blaze Hearing Statement at 7; Schneider, *supra* note 3.

location within three meters.[14] Upon law enforcement request, service providers can remotely and covertly activate the phone's GPS functionality and then cause the phone to transmit its coordinates back to the provider.[15]

B. Americans Believe the Data on and Generated by their Cellphones are Private

For the Fourth Amendment to apply, a person must "exhibit[] 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 cellphones, including location information. In 2014, the Pew Research Center reported that 82% of Americans consider the details of their physical location over time to be sensitive information—more than the proportion of respondents who considered as sensitive their relationship history, religious or political views, or their text messages.[16] In 2012, the Pew Center found that cellphone owners take a number of steps to protect access to personal information and mobile data, and more than half of phone owners with mobile apps have uninstalled or decided to not

---

[14] This is sometimes referred to as Assisted GPS or A-GPS. Jari Syrjärinne & Lauri Wirola, *Quantifying the Performance of Navigation Systems and Standards for Assisted-GNSS*, InsideGNSS, Sept./Oct. 2008, *available at* http://www.insidegnss.com/node/769; *What is GPS?*, Garmin, http://www8.garmin.com/aboutGPS/.

[15] If a phone is unable to calculate its GPS coordinates, the service provider will "fall back" to network-based location calculation. Third Notice at *40 n.306. Network-based technologies use existing cell site infrastructure to identify and track location by silently "pinging" the phone and then triangulating its precise location based on which cell sites receive the reply transmissions. Blaze Hearing Statement at 12; Pell & Soghoian, 27 Berkeley Tech. L. J. at 128.

[16] Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 34, 36-37 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (50% of respondents believed location information was "very sensitive.").

install an app due to concerns about the privacy in their personal information.[17] In addition, more than 30% of smart phone owners polled took affirmative steps to safeguard privacy: 19% turned off location tracking on their phones and 32% cleared their browsing or search history.[18] The numbers are higher for teenagers, with Pew reporting 46% of teenagers turned location services off.[19] A 2013 survey conducted on behalf of the Internet company TRUSTe found 69% of American smartphone users did not like the idea of being tracked.[20] And a 2009 Carnegie Mellon survey of perceptions about location-sharing technologies showed that participants believed the risks of these technologies outweighed the benefits and were "extremely concerned" about controlling access to location information.[21]

C. Americans' Subjective Expectation of Privacy in Cellphone Data is Objectively Reasonable

A court must necessarily look to "societal understandings" of what should be considered private to determine whether a subjective expectation of privacy is "reasonable" under the Fourth Amendment. *Oliver v. United States*, 466 U.S. 170,

---

[17] Jan Lauren Boyles et al., *Privacy and Data Management on Mobile Devices*, Pew Research Internet & American Life Project (Sept. 5, 2012), http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.

[18] *Id*.

[19] Kathryn Zickuhr, *Location-Based Services*, Pew Research Internet and American Life Project (Sept. 12, 2013), http://www.pewinternet.org/2013/09/12/location-based-services/.

[20] David Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTe Blog (Sept. 5, 2013), http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size/.

[21] 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.

178 (1984). 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 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). Courts and legislatures' progress toward protecting cellphone location data against warrantless searches underlines the reasonableness of the privacy expectation in this information.

1. *Courts Recognize the Privacy Implications of Location Information*

Courts around the country have recognized the privacy implications of location information. In 2012, a majority of Supreme Court Justices opined in *Jones* that people expect their otherwise public movements on the street to remain private. 132 S.Ct. 945. Although the Court ultimately held that placing a GPS tracking device on a car was a "search" because it was a physical trespass onto private property for purposes of obtaining information, *id.* at 949, in two separate concurring opinions, five members of the Court recognized that longer-term GPS location tracking "impinges on expectations of privacy." *Id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in the judgment). The other four

Justices did not dispute this conclusion; they simply did not address it. *Id.* at 953-54. In concluding that extended location tracking invades a person's 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). Likewise, Justice Alito wrote that "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 in the judgment).[22]

Following *Jones*, in 2014 the Supreme Court specifically cited location privacy as a reason to limit police searches of cellphones incident to arrest. *Riley v. California*, 134 S.Ct. at 2473, 2490 (2014). The Court explained that cellphones 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

---

[22] The fact that the instant case involved one day of tracking does not provide a basis for distinguishing it from *Jones* and subsequent cases. As the Florida Supreme Court has explained:

> basing the determination as to whether warrantless real time cell site location tracking violates the Fourth Amendment on the length of the time the cellphone is monitored is not a workable analysis. It requires case-by-case, after-the-fact, ad hoc determinations whether the length of the monitoring crossed the threshold of the Fourth Amendment in each case challenged. The Supreme Court has warned against such an ad hoc analysis on a case-by-case basis . . . .

Tracey v. State, 152 So.3d 504, 520 (Fla. 2014) (citing *Oliver,* 466 U.S. at 170). Because law enforcement will generally not know ahead of time how long the tracking will last, a warrant should be required as a categorical matter.

town but also within a particular building." *Id.* (citing *Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring)).

In the wake of *Jones*, many other courts have also recognized the privacy implications of location information. In *Commonwealth v. Augustine*, the Massachusetts Supreme Judicial Court held that historical cell site data may raise even greater privacy concerns than GPS tracking of cars because cell 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).

Likewise, in *State v. Earls*, the New Jersey Supreme Court distinguished cellphone location data from the data generated by older, less sensitive tracking devices like beepers. 70 A. 3d 630 (N.J. 2013). *Earls* held that cellphone location information blurs "the historical distinction between public and private areas . . . [and thus] does more than simply augment visual surveillance in public areas." *Id.* at 642-43 (citing *United States v. Knotts,* 460 U.S. 276, 282 (1983)). In *Tracey v. State*, the Florida Supreme Court held that "the use of [a person's] cell site location information emanating from his cellphone in order to track him in real time [is] a search within the purview of the Fourth Amendment for which [a] probable cause [warrant is] required." 152 So.3d 504, 526 (Fla. 2014). The court explained that "the ease with which the government, armed with current and ever-expanding technology, can now monitor and track our cellphones, and thus ourselves, with minimal expenditure of funds and manpower, is just the type of 'gradual and silent encroachment' into the very details of our lives that we as a society must be vigilant

to prevent." *Id.* at 522 (quoting James Madison, Speech in the Virginia Ratifying Convention on Control of the Military (June 16, 1788)).

Indeed, numerous federal and state courts have held that the Fourth Amendment requires law enforcement to obtain a warrant to access historical CSLI[23] or to conduct real-time tracking.[24] Also, many state courts have interpreted their state constitutions to require police to get a warrant or other court order to obtain phone records,[25] which would include records about a subscriber's location.

2. *A Growing Number of States Protect Location Information by Statute*

Given the broad national consensus among the American public that a person's physical movements and whereabouts are private, it is no surprise that a

---

[23] *See, e.g., United States v. Graham*, 796 F.3d 332, 360 (4th Cir. 2015), *rehearing en banc granted*, 2015 WL 6531272 (2015); *In re Application for Tel. Info.*, 2015 WL 4594558, *12 (N.D. Cal. 2015), *appeal filed*, No. 15-16760 (9th Cir. 2015); *United States v. Cooper*, 2015 WL 881578, *8 (N.D. Cal. 2015); *but see United States v. Davis*, 785 F.3d 498, 518 (11th Cir. 2015) (en banc), *cert. denied*, 2015 WL 4600402 (2015); *In re Application for Cell Site Data*, 724 F.3d 600 (5th Cir. 2013).

[24] *See, e.g., United States v. White*, 62 F. Supp. 3d 614, 622-23 (E.D. Mich. 2014); *United States v. Powell*, 943 F. Supp. 2d 759, 776-79 (E.D. Mich. 2013); *In re Application for an Order Authorizing Disclosure of Location Information for a Specified Wireless Telephone*, 849 F. Supp. 2d 526, 539–43 (D. Md. 2011); *see also Commonwealth v. Rushing*, 71 A.3d 939, 961-64 (Pa. Super. Ct. 2013) (so holding under the Pennsylvania Constitution), *rev'd on other grounds,* 99 A.3d 416 (Pa. Sup. Ct. 2014); *In re Application Relating to Target Phone*, 733 F. Supp. 2d 939 (N.D. Ill. 2009) (so holding under federal statutes); *but see United States v. Skinner*, 690 F.3d 772, 774 (6th Cir. 2012) (finding no reasonable expectation of privacy in shorter-term cellphone location data).

[25] *See, e.g., People v. Blair*, 602 P.2d 738, 746 (Cal. 1979); *People v. Sporleder*, 666 P.2d 135, 141-43 (Colo. 1983); *Shaktman v. State*, 553 So.2d 148 (Fla. 1989); *State v. Rothman*, 779 P.2d 1, 7-8 (Haw. 1989); *State v. Thompson*, 760 P.2d 1162, 1165-67 (Idaho 1988); *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). *See also Ellis v. State*, 353 S.E.2 19 (Ga. 1987) (interpreting state statute to require warrant to obtain phone records).

growing number of states—including Wisconsin, where Appellant was arrested—now protect privacy in location information through state law.

Within the Seventh Circuit, Wisconsin, Indiana, and Illinois all now require police to get a warrant to conduct real-time cellphone location tracking.[26] In advocating for Wisconsin's law, Senator Glenn Grothman, the bill's co-sponsor, recognized the need to protect "individual privacy rights during police investigations" and recommended that Wisconsin "be among the states leading the nation in addressing these important issues of privacy."[27] Senator Daniel Biss, lead sponsor of Illinois' law, which had unanimous support in the legislature, recognized that location information "can reveal a surprising amount of detailed information most of us believe should stay private," and stated that "a free society needs to put strict limits on the government's collection of information about citizens' private lives."[28] After Indiana Governor Mike Pence signed that state's bill into law, the bill's author, Representative Eric Koch, stated: "[w]ith technology continuing to evolve faster than the law, it was crucial to take steps to give all Hoosiers the peace of mind that common and reasonable expectations of privacy are still guaranteed

---

[26] See 725 Ill. Comp. Stat. 168/10; Ind. Code § 35-33-5-12; Wis. Stat. § 968.373(2). Wisconsin's statute was enacted in April 2014, after the search in this case.
[27] Testimony of Sen. Grothman (Dec. 19, 2013), *available at* http://lc.legis.wisconsin.gov/comtmats2013/ab0536.pdf. *See also* Testimony of Rep. Hutton (stating the law was needed to "provide appropriate privacy protections for law abiding citizens"), available at same link.
[28] Statement of Sen. Biss (Feb. 19, 2014), *available at* http://senatorbiss.com/component/content/article?id=82:biss-qmore-green-lightsq. *See also* legislative history of S.B. 2808, *available at* http://ilga.gov/legislation/BillStatus.asp?DocNum=2808&GAID=12&DocTypeID=SB&LegId=78729&SessionID=85&GA=98.

in Indiana."[29]

At least nine other states—California, Maine, Maryland, Minnesota, Montana, New Hampshire, Utah, Virginia, and Washington—also require police to get a warrant to conduct real-time cellphone location tracking.[30] Six of those states further require a warrant for historical cell site location information.[31]

State legislatures in other jurisdictions have enacted additional statutory protections for location information. At least seven states require police to get a warrant to install an electronic tracking device, [32] and at least seven states prohibit anyone, besides police, from using an electronic tracking device to monitor the movement of another person or their vehicle.[33]

The prevalence of state laws protecting location information shows that society accepts as reasonable a privacy interest in this information.

In sum, there has never been a higher number of people in the United States who have been promised by court decision or legislation that information about where they are or have been is private. The growing number of people protected by

---

[29] Statement of Rep. Koch (April 22, 2014), *available at* http://www.indianahouserepublicans.com/news/press-releases/r65-rep.-koch-s-privacy-bill-signed-into-law-4-22-2014/.
[30] Cal. Penal Code § 1546; 16 Maine Rev. Stat. § 648; Md. Code, Criminal Procedure 1-203.1(b)(1); Minn. Stat. §§ 626A.28(3)(d), 626A.42(1)(d); Mont. Code § 46-5-110(1)(a); N.H. Stat. § 644-A; Va. Code § 19.2-56.2; Wash. Rev. Code § 9.73.260.
[31] *See* Cal. Penal Code § 1546; 16 Maine Rev. Stat. § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(1)(d); Mont. Code § 46-5-110(1)(a); N.H. Stat. § 644-A.
[32] See Fla. Stat. § 934.42; Haw. Rev. Stat. § 803-44.7(b); Iowa Code § 808.4; Okla. Stat. Title 13, § 177.6(A); Or. Rev. Stat. § 133.619(6); 18 Pa. Stat. § 5761(c)(4); S.C. Code § 17-30-140(B)(2).
[33] See Cal. Penal Code § 637.7; Del. Code § 1335(a)(8); Haw. Rev. Stat. § 803-42(a)(8); Minn. Stat. § 626A.35; Tenn. Code § 39-13-606; Tex. Penal Code § 16.06; Va. Code § 18.2-60.5.

a warrant requirement, while not dispositive of whether there is a Fourth Amendment expectation of privacy in cellphone data, is compelling proof of "societal understandings" as to what level of privacy and security is reasonable.

II. An Expectation of Privacy in Cellphone Data Is Objectively Reasonable Even Though the Data Is Obtained by a Phone Company

An expectation of privacy in cellphone location information is not defeated simply because this location information is obtained by the telephone company. The government has frequently relied on the Supreme Court's opinion in *Smith v. Maryland*, 442 U.S. 735 (1979) — ruling there was no expectation of privacy in the phone numbers a person dials—to argue that cellphone users have no expectation of privacy in their data because it has been exposed to a third party. *See, e.g.* En Banc Brief of the United States, *United States v. Davis*, 2014 WL 7232613, at *11 (11th Cir. Dec. 17, 2014); *In re Application of U.S. for Site Data*, 724 F.3d 600, 612-13 (5th Cir. 2013); Brief of Appellee United States, *United States v. Graham*, 2013 WL 5538613, 46-47 (4th Cir. Oct. 8, 2013). But *Smith* does not alter the calculus here for several reasons.

First, the data here are significantly more revealing than the limited three days' worth of call records at issue in *Smith*. The Supreme Court in *Riley* recognized that cellphones 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 analog in the physical world. 134 S.Ct. at 2490-91. When the government argued in *Riley* that cellphones

are "materially indistinguishable" from physical items like a pack of cigarettes, the Court refused to equate the two. *Riley*, 134 S.Ct. at 2488-89. It believed comparing a search of all data on a cellphone 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 location data derived from a cellphone is so much vaster in quantity and intrusive in quality than the limited data generated by a simple landline phone, this Court cannot rely on cases that precede the digital revolution to determine how to protect cellphone data. *Id*. at 2488-89. Following *Riley*, this Court should adopt the same approach, taking cellphone location information for what it is—data that paints a rich and revealing portrait of an individual's life, movements, and associations—rather than relying on cases involving distinguishable and primitive technologies and less invasive government action.

Second, *Smith* does not reflect the realities of modern society. We share much more information about ourselves with third parties merely as a byproduct of 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-copies; or buying and reading books on our phones or Kindles instead of purchasing a physical book at a bookstore to read later at home. 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." 132 S.Ct. at 957 (Sotomayor, J., concurring). Homing 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.*[34]

Third, *Smith* held that there was no reasonable expectation of privacy in dialed phone numbers in part because the caller "voluntarily convey[s] numerical information to the telephone company." 442 U.S. at 744. The Third Circuit has explained why cellphone users retain a reasonable expectation of privacy in their historical cellphone location information under this "voluntariness" rubric:

> A cellphone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cellphone customers are aware that their cellphone providers *collect* and store historical location information. Therefore, "[w]hen a cellphone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cellphone user receives a call, he hasn't voluntarily exposed anything at all."

In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 318-19 (3d Cir. 2010) (alteration in original); *accord Graham*, 796 F.3d at 355 (citing Third Circuit's opinion). If

[34] *Smith* itself recognized that there may be situations where "an individual's subjective expectations [have] been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms," such as where the individual knows or believes that his activities are being monitored in ways that do not comport with the Fourth Amendment. In those situations, however, the individual's "subjective expectations obviously could play no meaningful role in ascertaining what the scope of the Fourth Amendment protection was. In determining whether a 'legitimate expectation of privacy' exist[s] in such cases, a normative inquiry would be proper." *Smith*, 442 U.S. at 741 n.5. *Accord Tracey*, 152 So.3d at 525-26 (applying "the 'normative inquiry' envisioned in *Smith*" to cellphone location tracking).

anything, this rationale applies with even greater force here. See Tracey, 152 So.3d at 522-23. In cases of real-time cellphone location tracking, the government initiates the gathering of data by directing the service provider to identify the present location of a phone, meaning that the data at issue would not have existed but for the government's action. The government's argument can only be that people give up any reasonable expectation of privacy simply by owning a phone, despite never intentionally, affirmatively, or knowingly disclosing their location. But forcing people to discard or turn off their cellphones "just to assure privacy from governmental intrusion that can reveal a detailed and intimate picture of the user's life places an unreasonable burden on the user to forego necessary use of his cellphone, a device now considered essential by much of the populace." Id. at 523.

Moreover, there are significant barriers to cellphone users understanding or controlling when their location information is, or even could be, tracked. As discussed above, many smartphones include location privacy settings that, when enabled, prevent apps from accessing the phone's location. However, these settings have no impact upon carriers' ability to determine the phone's location, giving phone users a false sense of privacy. Thus, "even though a user may demonstrate a subjective expectation of privacy by disabling an app's location identification features, that user's cellphone will still generate CSLI" accessible to the service provider. *In re Application*, 2015 WL 4594558, at *11. Similarly, the vast majority of location requests made by smartphone apps are invisible to users,[35] meaning that

[35] Primal Wijesekera, *et al.*, *Android Permissions Remistified: A Field Study on Contextual Integrity*, Proceedings of the 24th USENIX Security Symposium 505 (Aug. 2015), https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-

users have neither knowledge nor control over much of the location tracking to which their phone may be subjected. Cellphone location tracking at the request of the government is a far cry from the collection of dialed telephone numbers at issue in *Smith*. Ultimately, *Smith* is distinguishable from and does not control the outcome of this case. Just because technology is *capable* of disclosing to a third party 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.

III. The Government May Have Used a Stingray to Locate the Defendant

Although the affidavits in this case supporting the request for a pen register/trap and trace order state that the government sought to obtain cellphone location information from Sprint, the government may instead have located the Defendant using a cell-site simulator, commonly known as a Stingray.[36] If so, this lack of candor with the lower court and with the Defendant would be sufficient grounds to invalidate the order and to suppress the evidence gathered as a result of the unlawful search. *See Brady v. Maryland*, 373 U.S. 83 (1963).

---

paper-wijesekera.pdf ("We observed that fewer than 1% of location requests were made when the applications were visible to the user or resulted in the displaying of a GPS notification icon.").

[36] "StingRay" is the name for one cell-site simulator model sold by the Harris Corporation. *See* Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, Ars Technica, Sept. 23, 2013, http://bit.ly/1mkumNf. Cell-site simulators are also called "IMSI catchers," in reference to the unique identifier—or international mobile subscriber identity—of wireless devices that they track. Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J.L. & Tech. 1, 11 (2014).

Cell-site simulators are privacy-invasive devices that have been employed by law enforcement agencies for years with little to no oversight from legislative bodies or the courts due to an intentional governmental policy of secrecy. Cell-site simulators can be carried by hand, installed in vehicles, or mounted on aircraft. The devices masquerade as the cellular tower antennas used by wireless companies such as Sprint, and in doing so, force all mobile phones within range that subscribe to the impersonated wireless carrier to emit identifying signals, which can be used to locate not only a particular suspect, but countless bystanders as well.

Law enforcement agencies around the country have attempted to hide their use of Stingrays from defendants, prosecutors, and even from the courts. In discussing the Baltimore Police Department's use of Stingrays, *USA Today* noted that "[i]n court records, police routinely described the phone surveillance in vague terms—if they mentioned it at all."[37] In some cases "the police merely said they had 'located' a suspect's phone without describing how, or they suggested they happened to be in the right place at the right time."[38] Similarly, in Tacoma, Washington, law enforcement officers used Stingrays without disclosing their use to defense attorneys, the prosecutor's office, or even superior court judges,[39] and in Sacramento, California, in hundreds or thousands of cases police "never told judges or prosecutors that they were using the so-called 'cell site simulators'—nor did they

---

[37] Brad Heath, "Police secretly track cellphones to solve routine crimes," *USA Today* (Aug. 24, 2015) http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

[38] *Id.*

[39] Kate Martin, "Documents: Tacoma police using surveillance device to sweep up cellphone data," *The News Tribune* (Aug. 26, 2014). http://www.thenewstribune.com/news/local/article25878184.html.

specifically ask for permission to use one."[40] In Sarasota, Florida, at the request of the United States Marshals, police officers intentionally hid the use of Stingrays from criminal defendants, and referred in court filings to the use of a Stingray as "receiv[ing] information from a confidential source regarding the location of the suspect."[41] Prosecutors have even withdrawn evidence rather than allow testimony in court about Stingrays.[42]

The government may have tried to hide its use of a Stingray here. As Magistrate Judge Callahan's Order notes, the government failed to disclose in any of its reports that it had located the Defendant by tracking his cellphone, and the Defendant did not learn about this fact until an evidentiary hearing on February 4, 2014. *See* App. 010 (Recommendation on Defendant's Motion to Suppress Evidence, p. 3, n.1 (Sept. 30, 2014)). Similar to officers' attempts to obfuscate Stingray use in other jurisdictions, the officers here stated they "'obtained information' of Patrick's location; . . . had 'prior knowledge' that Patrick was occupying the vehicle; . . . [and] 'obtained information from an unknown source' that Patrick was inside the vehicle at that location." *Id.* Even at the evidentiary hearing where officers admitted to

---

[40] *New Developments in Sacramento "Stingray" Case*, ABC 10 (Jan. 8, 2016), http://www.abc10.com/story/news/local/sacramento/2016/01/08/new-developments-sacramento-stingray-case/78541240/.

[41] Email from Sergeant Kenneth Castro, Sarasota Police Department (April 15, 2009) released in response to a public records request and *available at* https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf.

[42] Justin Fenton, "Judge threatens detective with contempt for declining to reveal cellphone tracking methods," *Baltimore Sun* (Nov. 17, 2014) http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html.

cellphone tracking, they would only acknowledge they received "electronic information" confirming the Defendant was in the vehicle. Transcript, Evidentiary Hearing, Dkt. No. 32, pp. 29-30 (Feb. 4, 2014). When Patrick's attorney asked what "electronic information" meant, the officer would only say that it involved "tracking [a] cell phone." *Id.* at 34, 35-36.

Logs from the Milwaukee Police Department, released in response to a public records request, suggest that the agency may have used a cell-site simulator to locate the Defendant.[43] These logs state that the agency used a Stingray to locate a "fugitive" "related to [an] FBI roundup" on October 28, 2013.[44] According to Judge Callahan's Order, the FBI was involved in locating the Defendant in this case, and he was apprehended on October 28, 2013. App. 011 (Order at 3-4 (citing Officer Mark Harms' affidavit)).

It would not be surprising if the Milwaukee Police Department failed to disclose that it had used a Stingray in this case. On August 13, 2013, the Department signed a non-disclosure agreement with the FBI concerning its use of Stingrays.[45] In the document, the Department agreed to "not, in any civil or

---

[43] *See* Open Records Request from Mike Katz-Lacabe (Aug 3, 2015) *available at* http://www.cehrp.org/wp-content/uploads/2016/01/Milwaukee_PD_NDA_approval_request_3Aug2015.pdf; Milwaukee Police Department Letter in Response to Records Request (Sept. 21, 2015) *available at* https://assets.documentcloud.org/documents/2696663/Milwaukee-PD-StingRay-Response-21Sep2015.pdf.

[44] Log Documenting the Use of Cellular Telephone Surveillance Equipment, 4 *available at* http://www.cehrp.org/wp-content/uploads/2015/09/Milwaukee_PD_StingRay_use_log_Sep2015.pdf.

[45] Letter from FBI Re: Acquisition of Wireless Collection Equipment/Technology and NonDisclosure Obligations (Aug. 13, 2013) *available at*

criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology . . . beyond the evidentiary results obtained through the use of the equipment/technology." This prohibition covers disclosure in all manner of judicial documents and proceedings, including "during pre-trial matters, in search warrants and related affidavits, in discovery" or at trial. Incredibly, the Department even agreed to "at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology. . . beyond the evidentiary results obtained through the use of the equipment/technology."[46]

It is not dispositive that the government's affidavit submitted in support of the application for a pen/trap order and the application itself state that the data would be obtained from Sprint or another carrier.[47] In a criminal case now on appeal in Maryland, *State v. Andrews*, No. 1496 (Md. Ct. Spec. App.), Baltimore Police officers also requested and were granted a pen/trap order seeking information from named cellphone service providers to track a suspect.[48] However, the defendant in that case later learned the police department had used data from the carrier to identify the general location of the phone, and then used a Stingray to

---

https://assets.documentcloud.org/documents/2190206/milwaukee-pd-fbi-nda-13aug2013.pdf.

[46] *Id*.

[47] *See* App. 028, 030-031.

[48] *See* Application of Detective Michael Spinnato, In the Matter of an Application of the State of Maryland for an Order Authorizing the Installation and Use of a Device Known as a Pen Register/Trap & Trace (May, 5, 2014) *available at* https://www.eff.org/files/2015/12/29/andrews_dnr_app-order.pdf.

pinpoint it within a specific home. Baltimore officers eventually testified that they had used the device to find the defendant, specifically not disclosed it in any report filed about the defendant's arrest, and failed to inform the State's Attorney that a Stingray had been used.[49] The judge concluded the police officers intentionally withheld this information.[50] At a later hearing on the defendant's motion to suppress, another judge concluded the pen register order did not authorize the use of a Stingray because a Stingray operates in a manner fundamentally different from the collection of location information from a cellphone service provider.[51] Given this, the judge held the use of the device violated the Fourth Amendment and that the good-faith exception did not apply. She suppressed all information generated from the use of the device and all evidence gathered after the device was used.[52]

Cell-site simulators raise especially serious questions under the Fourth Amendment, and at least require a warrant. Use of a cell-site simulator constitutes a search for several reasons. First, the device can precisely locate and track people's phones, which requires a warrant for the same reasons that tracking by the service provider does. Second, cell-site simulators transmit probing electronic signals through the walls of homes, offices, and other private spaces occupied by the target and innocent third parties in the area, and thereby force phones to transmit data to the government that reveals where inside those spaces the phones are. By

---

[49] *See* Transcript, *State v. Andrews*, 61-62, 86 (June 4, 2015), *available at* https://www.eff.org/files/2015/12/29/andrews_june_4_2015_transcript.pdf
[50] *Id.* at 97.
[51] *See* Transcript, *State v. Andrews,* 36-37 (Aug. 20, 2015), *available at* https://www.eff.org/files/2015/12/29/andrews_aug_20_2015_transcript.pdf.
[52] *Id.* at 48-49, 53.

pinpointing suspects and third parties while they are inside constitutionally protected spaces, cell-site simulators invade reasonable expectations of privacy. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (thermal imaging to detect heat from home constituted search); *United States v. Karo*, 468 U.S. 705, 715 (1984) (monitoring of radio-location beeper that was taken into residence constituted search). Third, cell-site simulators search the contents of people's phones by forcing those phones to transmit their electronic serial number and other identifying information in electronic storage on the device. Searching the contents of a cellphone requires a warrant. *Riley*, 134 S.Ct. 2473. Fourth, cell-site simulators significantly impact third parties. Even when the government is using a cell-site simulator with the intent to locate or track a particular suspect, the device unavoidably forces bystanders' phones in the area to transmit their unique electronic serial numbers, thus signaling their identities and locations.

Even with a warrant, this closely resembles the kind of dragnet search and general warrant about which the Framers of the Fourth Amendment were so concerned. *See Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). Assuming that such dragnet searches are ever permissible, they must at least be constrained by a warrant based on probable cause that mandates minimization of innocent parties' data and other protections. *In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *3–4 (N.D. Ill. Nov. 9, 2015) (mandating protections for innocent third parties in issuance of cell-site simulator warrants); *cf. Berger v. New York*, 388 U.S. 41, 57–59 (1967) (similar protections for wiretaps).

If the government did, in fact, use a Stingray in this case and failed both to disclose this fact to the judge who issued the pen/trap order and to the Defendant, this would be sufficient grounds for suppressing the evidence gathered as a result of using the device.

CONCLUSION

For the foregoing reasons, this Court should hold that real-time cellphone location tracking is a Fourth Amendment search. Americans have a reasonable expectation of privacy in the location data generated by their phones, and, as the Court held 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: January 22, 2016

By: /s/ Adam Schwartz

Adam Schwartz
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Fl.
New York, NY 10004

Laurence J. Dupuis
ACLU OF WISCONSIN, INC.
207 E. Buffalo St., #325
Milwaukee, WI 53202

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

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

1. This Brief Amici Curiae of Electronic Frontier Foundation, American Civil Liberties Union Foundation, and ACLU of Wisconsin, Inc. complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,954 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 Word 2011 in 12-point Century Schoolbook.

Dated: January 22, 2016

By: */s/ Adam Schwartz*
Adam Schwartz
Counsel for Amici Curiae

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 Seventh Circuit by using the appellate CM/ECF system on January 22, 2016.

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: January 22, 2016

By: */s/ Adam Schwartz*
Adam Schwartz
Counsel for Amici Curiae