NO. 12-12928-EE

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff/appellee,

v.

QUARTAVIOUS DAVIS,
Defendant/appellant.

On Appeal from the United States District Court
for the Southern District of Florida

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF FLORIDA, INC., CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS*

Maria Kayanan
mkayanan@aclufl.org
Fla. Bar No. 305601
ACLU Foundation of Florida, Inc.
4500 Biscayne Blvd. Ste. 340
Miami, FL 33137
Tel: 786-363-2700
Fax: 786-363-3108

Nathan Freed Wessler (*admission pending*)
nwessler@aclu.org
Catherine Crump
Ben Wizner
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel: 212-549-2500
Fax: 212-549-2654

*Unopposed Motion for Leave to File Late Amicus Brief Pending

Benjamin James Stevenson
bstevenson@aclufl.org
Fla. Bar No. 589909
ACLU Foundation of Florida, Inc.
P.O. Box 12723
Pensacola, FL 32591-2723
Tel: 786-363-2738
Fax: 786-363-1985

Kevin S. Bankston
Gregory T. Nojeim
Center for Democracy & Technology
1634 I St NW, Suite 1100
Washington, DC 20006
(202) 637-9800

Hanni Fakhoury
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

David Oscar Markus
Vice-Chair, 11th Circuit Amicus Committee
Nat'l Ass'n of Criminal Defense Lawyers
Markus & Markus, PLLC
40 N.W. 3rd Street,
Penthouse One
Miami, Florida 33128
Tel: (305) 379-6667
Fax: (305) 379-6668
dmarkus@markuslaw.com

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

United States v. Quartavious Davis
No. 12-12928

Amici Curiae file this Certificate of Interested Persons and Corporate Disclosure Statement, as required by Local Rules 26.1-1, 28-1(b), and 29-2.

Altman, Roy, Assistant United States Attorney

American Civil Liberties Union Foundation, *Amicus Curiae*

American Civil Liberties Union Foundation of Florida, Inc., *Amicus Curiae*

Bankston, Kevin, Counsel for Center for Democracy & Technology

Brown, Hon. Stephen T., United States Magistrate Judge

Caruso, Michael, Interim Federal Public Defender

Center for Democracy & Technology, *Amicus Curiae*

Colan, Jonathan, Assistant United States Attorney

Crump, Catherine, Counsel for *Amici Curiae*

Davis, Quartavious, Defendant/Appellant

Dube, Hon. Robert L., Untied States Magistrate Judge

Electronic Frontier Foundation, *Amicus Curiae*

Fakhoury, Hanni, Counsel for Electronic Frontier Foundation

Ferrer, Wifredo A., United States Attorney

Fisher, Sylvester, Co-Defendant

Garber, Hon. Barry L., United States Magistrate Judge

Gold, Hon. Alan S., United States District Judge

Golembe, Stephen J., Co-Defendant Counsel

Kayanan, Maria, Counsel for *Amici Curiae*

Korchin, Paul M., Assistant Federal Public Defender

Lenard, Hon. Joan A., United States District Judge

Malone, Omar, Co-Defendant Counsel

Markus, David Oscar, Counsel for Nat'l Ass'n of Criminal Defense Lawyers

Martin, Michael, Co-Defendant

Martin, Jahmal A., Co-Defendant

McAliley, Hon. Chris M., United States Magistrate Judge

Michaels, Alexander J., Co-Defendant Counsel

Moss, Jr., Reginald A., Co-Defendant Counsel

National Association of Criminal Defense Lawyers, *Amicus Curiae*

Nojeim, Greg, Counsel for Center for Democracy & Technology

O'Sullivan, Hon. John J., United States Magistrate Judge

Palermo, Hon. Peter R., Untied States Magistrate Judge

Perwin, Amanda, Assistant United States Attorney

Reid, Jamarquis T., Co-Defendant

Schultz, Anne R., Assistant United States Attorney

Shapiro, Jacqueline E., Appellate Counsel

Sibila, Jorge A., Co-Defendant Counsel

Smith, Willie, Co-Defendant

Stevenson, Benjamin James, Counsel for *Amici Curiae*

Torres, Hon. Edwin G., United States Magistrate Judge

Turnoff, Hon. William C., United States Magistrate Judge

Ungaro, Hon. Ursula, United States District Judge

Wessler, Nathan Freed, Counsel for *Amici Curiae*

White, Hon. Patrick A., United States Magistrate Judge

Wizner, Ben, Counsel for *Amici Curiae*

Williams, Hon. Kathleen M., United States District Judge

Zelman, Michael, Trial Counsel

Corporate Disclosure Statement

Amici Curiae American Civil Liberties Union Foundation, American Civil Liberties Union Foundation of Florida, Inc., Center for Democracy & Technology, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers are non-profit entities that do not have parent corporations. No publicly held corporation owns 10 percent or more of any stake or stock in *amici curiae*.

/s/ Maria Kayanan

Maria Kayanan

STATEMENT REGARDING ORAL ARGUMENT

Amici curiae submit that oral argument is appropriate in this case because the Fourth Amendment question on appeal is an issue of first impression in this Circuit. *Amici curiae* respectfully seek leave to participate in oral argument on the Fourth Amendment question, because their participation may be helpful to the Court in addressing the novel and important issues presented by this appeal. *See* Fed. R. App. P. 29(g).

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases

Other Authorities

INTEREST OF AMICI CURIAE[1][2]

The American Civil Liberties Union Foundation ("ACLU") is a nationwide nonpartisan organization of nearly 500,000 members, dedicated to protecting the fundamental liberties and basic civil rights guaranteed by state and federal Constitutions. The ACLU of Florida, a state affiliate of the national ACLU, is devoted to advocacy on behalf of more than 18,000 statewide members and supporters. The ACLU and its affiliates, including the ACLU of Florida, are well-positioned to submit an *amicus* brief in this case. They have long been committed to defending individuals' Fourth Amendment rights and have been at the forefront of numerous state and federal cases addressing the right of privacy.

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

---

[1] Pursuant to Rule 29(a), counsel for *amici curiae* certifies that all parties have consented to the filing of this brief. Pursuant to Rule 29(c)(5), counsel for *amici curiae* states that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

[2] *Amici curiae* filed a motion to file amicus brief out of time on July 10, 2013, proposing a July 17, 2013 deadline for this brief. That motion is currently pending.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported organization based in San Francisco, California, that works to protect privacy and free speech rights in an age of increasingly sophisticated technology. As part of that mission, EFF has served as counsel or *amicus curiae* in many cases addressing Fourth Amendment issues raised by emerging technologies, including location-based tracking techniques such as GPS and collection of cell site tracking data. *See, e.g.*, *United States v. Jones*, 132 S. Ct. 945 (2012), *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010); *United States v. Jones*, 908 F. Supp. 2d 203 (D.D.C. 2012; *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010), *Commonwealth v. Rousseau*, --- N.E.2d ----, 465 Mass. 372 (2013).

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of approximately 10,000 direct members in 28 countries, and 90 state, provincial and local affiliate organizations totaling up to 40,000 attorneys. NACDL's members include private criminal defense lawyers, public defenders, military defense

counsel, law professors, and judges. NACDL files numerous amicus briefs each year in the Supreme Court, this Court, and other courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

STATEMENT OF THE ISSUES

1. Whether the government violated the Fourth Amendment when it obtained 67 days' worth of Defendant's cell phone location information without a warrant.
2. Whether the Court should address the Fourth Amendment issue regardless of whether it determines that the good faith exception to the exclusionary rule applies.

SUMMARY OF ARGUMENT

Location surveillance, particularly over a long period of time, can reveal a great deal about a person. "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 sub nom. United States v. Jones*, 132 S. Ct. 945 (2012). Accordingly, in *United States v. Jones*, five Justices of the Supreme Court concluded that an investigative subject's "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." 132 S. Ct. at 958, 964 (Alito, J. concurring in the judgment); *id.* at 955 (Sotomayor, J. concurring).

In this case, law enforcement obtained 67 days of cell site location information ("CSLI") for Defendant's phone without a warrant. If tracking a vehicle for 28 days in *Jones* was a search, then surely tracking a cell phone for 67 days is likewise a search, particularly because people keep their phones with them as they enter private spaces traditionally protected by the Fourth Amendment.

The district court denied Defendant's motion to suppress without explanation and without issuing a written opinion. D.E. 276; D.E. 277, at 45. The court's denial of the suppression motion fails to take account of five Justices'

determination that Americans have a reasonable expectation that they will not be subject to long-term and constant surveillance of their movements. Further, to the extent the district court relied on Supreme Court jurisprudence regarding bank records and dialed telephone numbers it erred, because cell phone location data is not voluntarily communicated to phone service providers, in contrast to the willful communication of banking transaction data and dialed numbers to banks and telecommunication companies. The government's acquisition of Defendant's comprehensive cell phone location information without a warrant violates the Fourth Amendment.

ARGUMENT

I. WARRANTLESS ACQUISITION OF LONG-TERM HISTORICAL CELL SITE LOCATION INFORMATION VIOLATED DEFENDANT'S REASONABLE EXPECTATION OF PRIVACY UNDER THE FOURTH AMENDMENT.

A. Defendant's Cell Site Location Information Obtained by the Government Reveals Invasive and Accurate Information About His Location and Movements Over Time.

i. Cell site location information reveals private, invasive, and increasingly precise information about individuals' locations and movements.

As of December 2012, there were 326.4 million wireless subscriber accounts in the United States, responsible for 2.30 trillion annual minutes of calls and 2.19

trillion annual text messages.[3] Cell phone use has become ubiquitous: the number of wireless accounts now exceeds the total population of the United States,[4] more than 83% of American adults own cell phones,[5] and one in three U.S. households has only wireless telephones.[6]

Cellular telephones regularly communicate with the carrier's network by sending radio signals to nearby base stations, or "cell sites." *The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and 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)[7] ["Blaze Hearing Statement"]. When turned on, "[c]ell phone handsets periodically (and automatically) identify themselves to the nearest base station (that with the strongest radio signal) as they move about the coverage area." *Id.* Phones communicate with the wireless network when a subscriber makes or receives calls or transmits or receives text messages. Smartphones, which are now used by more

---

[3] *U.S. Wireless Quick Facts*, CTIA – The Wireless Association, *available at* http://www.ctia.org/advocacy/research/index.cfm/aid/10323.
[4] *Id.*
[5] Aaron Smith, Pew Research Ctr., *Americans and Text Messaging* 2 (2011), *available at* http://pewinternet.org/~/media//Files/Reports/2011/Americans%20and%20Text%20Messaging.pdf.
[6] *U.S. Wireless Quick Facts*, *supra*.
[7] *Available at* http://judiciary.house.gov/hearings/113th/04252013/Blaze%2004252013.pdf.

than half of Americans,[8] communicate even more frequently with the carrier's network, because they typically check for new email messages every few minutes.[9] When phones communicate with the network, the service provider automatically retains information about such communications, which for calls includes which cell site the phone was connected to at the beginning and end of the call.[10] Most cell sites consist of three directional antennas that divide the cell site into sectors (usually of 120 degrees each),[11] but an increasing number of towers have six sectors.[12] Service providers automatically retain sector information too, which reveals even more precise information about the user's location.[13] In addition to

---

[8] Maeve Duggan & Lee Rainie, Pew Research Ctr., *Cell Phone Activities 2012* 12 (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_CellActivities_11.25.pdf.

[9] Gyan Ranjan et al., *Are Call Detail Records Biased for Sampling Human Mobility?*, Mobile Computing & Comm. Rev., July 2012, at 34, *available at* http://www-users.cs.umn.edu/~granjan/Reports/MC2R_2012_CDR_Bias_Mobility.pdf.

[10] Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 Berkeley Tech. L. J. 117, 128 (2012).

[11] Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Attorneys' Bull., Nov. 2011, at 16, 19, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

[12] D.E. 283, at 220. Examples of MetroPCS six-sector towers in the Miami area can be found throughout the master list of MetroPCS cell sites. *See, e.g.*, Ex. A, at BS003080–87 (switch Plantation1, tower 541; switch Plantation2, towers 3, 7, 10, 13, 20, 111, 119, 201, 202, 206, 207).

[13] The availability of historical cell site location information and the length of time it is stored depends on the policies of individual wireless carriers: Sprint/Nextel stores data for 18–24 months, T-Mobile for one year, and AT&T/Cingular indefinitely "from July 2008." U.S. Dep't of Justice, Retention Periods of Major

cell site and sector, some carriers also calculate and log the caller's distance from the cell site.[14]

The precision of a user's location revealed by the cell site identifier in the carrier's records depends on the size of the sector. The coverage area for a cell site is reduced in areas with greater density of cell towers, with the greatest cell site density and thus smallest coverage areas in urban areas. For example, a searchable database of publicly available information reveals that there are 60 towers and 759 antenna sites within a one-mile radius of the Eleventh Circuit's courthouse in Atlanta.[15] Similarly, there are 161 towers and 961 antenna sites within a three-mile radius of the Eleventh Circuit's satellite office in Miami.[16]

Cell site density is increasing rapidly, largely as a result of the growth of internet usage by smartphones. *See* CTIA – The Wireless Association, Semi-

---

Cellular Service Providers (Aug. 2010), *available at* https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart. MetroPCS retains CSLI for six months. MetroPCS, MetroPCS Subpoena Compliance, Attach. A to Letter from Steve Cochran, Vice President, MetroPCS Commc'ns, Inc., to Rep. Edward J. Markey (May 23, 2012), *available at* http://web.archive.org/web/20130318011325/http://markey.house.gov/sites/markey.house.gov/files/documents/MetroPCS%20Response%20to%20Rep.%20Markey.PDF.

[14] *See* Verizon Wireless Law Enforcement Resource Team (LERT) Guide 25 (2009), *available at* http://publicintelligence.net/verizon-wireless-law-enforcement-resource-team-lert-guide/ (providing sample records indicating caller's distance from cell site to within .1 of a mile).

[15] Search conducted using http://www.antennasearch.com.

[16] Search conducted using http://www.antennasearch.com.

Annual Wireless Industry Survey 2 (2012)[17] (showing that the number of cell sites in the United States has more than doubled in the last decade, with 285,561 as of June 2012); *id.* at 8 (wireless data traffic increased by 586% between 2009 and 2012). Each cell site can supply a fixed volume of data required for text messages, emails, web browsing, streaming video, and other uses. Therefore, the only way for providers to maintain adequate coverage as smartphone data usage increases is to erect more cell sites or add antennas to existing cell sites. As new cell sites are erected, the coverage areas around existing nearby cell sites will be reduced, so that the signals sent by those sites do not interfere with each other. *See* Ctr. for Democracy & Tech., Cell Phone Tracking: Trends in Cell Site Precision 2 (2013).[18]

In addition to erecting new conventional cell sites, providers are also able to increase their network coverage using low-power small cells, called "microcells," "picocells," and "femtocells," which provide service to areas as small as ten meters. *Id.* Femtocells are frequently provided by carriers directly to consumers with poor cell phone coverage in their homes or offices and the number of femtocells nationally now exceeds the number of traditional cell sites. *Id.* at 3.[19]

---

[17] *Available at* http://files.ctia.org/pdf/CTIA_Survey_MY_2012_Graphics-_final.pdf.

[18] *Available at* https://www.cdt.org/files/file/cell-location-precision.pdf.

[19] For example, Sprint and AT&T have each distributed approximately one million femtocells. Informa Telecoms & Media, *Small Cell Market Status* 4–5 (2013),

Because the coverage area of femtocells is so small, callers connecting to a carrier's network via femtocells can be located to a high degree of precision, "sometimes effectively identifying individual floors and rooms within buildings."[20] Blaze Hearing Statement at 12. Femtocells with ranges extending outside of the building in which they are located can also provide cell connections to passersby, providing highly precise information about location and movement on public streets and sidewalks.[21]

Each call or text message to or from a cell phone generates a location record,[22] and at least some, if not all, of those records will reveal information precise enough to know or infer where a person is at a number of points during the day:

---

available at http://www.smallcellforum.org/smallcellforum_resources/pdfsend01.php?file=050-SCF_2013Q1-market-status%20report.pdf. T-Mobile, which recently acquired MetroPCS, has deployed femtocells since 2010 in the UK and intends to deploy them in the US. *Id.* at App. 5, 8.

[20] Wireless providers are required by law to be able to identify the location of femtocells, both to comply with emergency calling location requirements (E-911), and to comply with federal radio spectrum license boundaries. *See* 3rd Generation Partnership Project 2, *Femtocell Systems Overview* 33 (2011), *available at* http://www.3gpp2.org/public_html/specs/S.R0139-0%20v1.0_Femtocell%20Systems%20Overview%20for%20cdma2000%20Wireless%20Communication%20Systems_20110819.pdf.

[21] Tom Simonite, *Qualcomm Proposes a Cell-Phone Network by the People, for the People*, MIT Tech. Rev. (May 2, 2013), *available at* http://www.technologyreview.com/news/514531/qualcomm-proposes-a-cell-phone-network-by-the-people-for-the-people/.

[22] The historical call records obtained in this case include cell site information for each of Defendant's calls, but not for his text messages. *See* D.E. 283, at 229.

> A mobile user, in the course of his or her daily movements, will periodically move in and out of large and small sectors. Even if the network only records cell tower data, the precision of that data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less precise. For a typical user, over time, some of that data will inevitably reveal locational precision approaching that of GPS.

Blaze Hearing Statement at 15. Importantly, when law enforcement requests historical CSLI, it too cannot know before receiving the records how precise the location information will be. Agents will not have prior knowledge of whether the surveillance target was in a rural area with sparse cell sites, an urban area with dense cell sites or six-sector antennas, or a home, doctor's office, or church with femtocells. Likewise, they will not know if a target had a smartphone that communicates with the carrier's network (and thus generates location data) every few minutes, or a traditional feature phone that communicates less frequently.

Knowing periodic information about which cell sites a phone connects to over time can also be used to interpolate the path the phone user traveled, thus revealing information beyond just the cell site sector in which the phone was located at discrete points.[23] Law enforcement routinely uses cell site data for this

[23] *See, e.g.* Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Syss. Design & Implementation 20 (2011), *available at* https://www.usenix.org/legacy/events/nsdi11/tech/full_papers/Thiagarajan.pdf?CFI

purpose; in this case, the government argued that cell site data points showing Defendant's locations leading up one of the robberies revealed a trajectory that placed him at the business in question at the relevant time. D.E. 285, at 37. Similar data could just as easily be used to conclude from cell site data points when a person visited their doctor's office or church.

ii. Defendant's location information obtained by law enforcement reveals voluminous and private information about his locations and movements.

In this case, the government obtained 67 days of cell site location information for Defendant and his alleged co-conspirators. The records reveal the cell site and sector in which the caller was located when each call began and ended, thus providing law enforcement with a dense array of data about these men's locations. *See* Ex. B; Gov't Trial Exs. 32–35 (call detail records for Jamarquis Reid, Willie Smith, Jahmal Martin, and Quartavious Davis).[24] Defendant's data include 5,803 separate call records for which CSLI was logged,

---

D=230550685&CFTOKEN=76524860 (describing one algorithm for accurate trajectory interpolation using cell site information).

[24] The cell site and sector information for the start and end of each call is found in the last six columns of the spreadsheets. The sixth-to-last column provides the routing switch for the cell site. The next two columns provide the sector and cell site the phone connected to at the start of the call; the last two columns provide the same information for the end of the call. D.E. 283, at 210–12, 224–25

comprising 11,606 cell site location data points.[25] Ex. B. Mr. Smith's and Mr. Martin's records reveal 5,676 and 3,668 calls for which location information was logged, respectively. Gov't Trial Exs. 33 & 34. Defendant placed or received an average of 86 calls per day for which location data was recorded and later obtained by the government.

This data is particularly revealing of location information because of the density of cell sites in the greater Miami area. MetroPCS, the carrier used by Defendant and his alleged co-conspirators, operated a total of 214 cell sites comprising 714 sector antennas within Miami-Dade County, and many more cell sites elsewhere in southern Florida, at the time Defendant's location records were obtained. *See* Ex. A. These figures may actually underrepresent the density of cell sites available to MetroPCS customers in southern Florida because the company has roaming agreements with other carriers, significantly expanding its coverage and the number of cell towers its users' phones may connect to.[26]

---

[25] The records include information about additional calls for which cell site location information was not logged, adding up to a total of 7,476 lines of data for Defendant.

[26] *See* MetroPCS Commc'ns, Inc., Form 10-K, Annual Report Pursuant to Section 13 OR 15(D) of the Securities Exchange Act of 1934 6 (2010), *available at* https://www.sec.gov/Archives/edgar/data/1283699/000119312511051403/d10k.htm; Samia Perkins, *MetroPCS May be the Biggest Winner in AT&T/T-Mobile Deal*, Slash Gear (Mar. 22, 2011), http://www.slashgear.com/metropcs-may-be-the-biggest-winner-in-attt-mobile-deal-22141766/ ("[MetroPCS] ha[s] been adept at securing roaming agreements to use competitor's networks . . . ."); Kevin Fitchard, *Leap, MetroPCS Make Nice*, Connected Planet (Sept. 30, 2008),

The records obtained by the government reveal many details about Defendant's locations and movements during the two months tracked. For example, Defendant's calls include location records from 55 towers and 113 separate sectors, and over the course of a typical day his records chart his movements between multiple sectors. On August 13, 2010, for example, he made and received 108 calls in 22 unique cell site sectors. Even records of individual calls provide information about movement: 378 of his calls were initiated within one cell site sector and terminated in another, suggesting that he was not stationary during the call. The records thus reveal a granular accounting of Defendant's movements over time.

The records also reveal information about particular locations visited. The most frequently occurring cell site and sector in Defendant's records (switch Plantation1, tower 129, sector 2), corresponds to his residence at that time. From August 1–20, 2010, the call records logged Defendant's location in that sector 2,134 times, providing strong indication of when he was in his home.[27] Over the whole 67-day period, 37 calls started in his home sector and ended elsewhere, and 131 calls started elsewhere and ended when he was in or near home, providing

---

http://connectedplanetonline.com/wireless/news/leap-metropcs-mutual-agreement-0930/; D.E. 283, at 234.

[27] This includes data points from both the start and end of calls.

information about his patterns of movement to and from home as well as his static location there.

The records also allow inferences about where Defendant slept, which could reveal private information about the status of relationships and any infidelities.[28] By sorting the data for the first and last calls of each day, one can infer whether a person slept at home or elsewhere.[29] For example, from August 2 to August 31, 2010, Defendant's last call of the night and first call of the morning were either or both placed from his home sector (2-129). But on September 1 and 2, 2010, both the last call of the night and the first call of the next morning were placed from a location in a neighboring community (sector 2 of cell site 400, switch Plantation2). This information, like that described above, is deeply sensitive and quintessentially private.

B. Obtaining 67 Days' Worth of Cell Phone Location Data Is a "Search" Under the Fourth Amendment Requiring a Warrant Based Upon Probable Cause.

The Supreme Court has made clear that when the government engages in prolonged location tracking, or when tracking reveals information about a private space that could not otherwise be observed, that tracking violates a reasonable

[28] *See* Jane Mayer, *What's the Matter with Metadata?*, New Yorker (June 6, 2013), http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html ("Such data can reveal, too, who is romantically involved with whom, by tracking the locations of cell phones at night.").

[29] The government actually conducted such an analysis in this case. D.E. 285, at 48–52.

expectation of privacy and therefore constitutes a search within the meaning of the Fourth Amendment. Acquisition of Defendant's cell phone location information is a search for both of these reasons. Because warrantless searches are "'*per se* unreasonable,'" the acquisition of Defendant's location records violated his Fourth Amendment rights. *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)).

In *United States v. Jones*, five Justices agreed that when the government engages in prolonged location tracking, it conducts a search under the Fourth Amendment. 132 S. Ct. at 964 (Alito, J.); *id.* at 955 (Sotomayor, J.). The case involved law enforcement's installation of a GPS tracking device on a suspect's vehicle and its use to track his location for 28 days. *Id.* at 948. Although the majority opinion relied on a trespass-based rationale to determine that a search had taken place, *id.* at 949, it specified that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* [reasonable-expectation-of-privacy] analysis." *Id.* at 953.

Five Justices conducted a *Katz* analysis, and concluded that longer-term location tracking violates reasonable expectations of privacy. *Id.* at 960, 964 (Alito, J.); *id.* at 955 (Sotomayor, J.). Justice Alito wrote that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 964. This conclusion did not depend on the particular type of

tracking technology at issue in *Jones*, and Justice Alito identified the proliferation of mobile devices as "[p]erhaps most significant" of the emerging location tracking technologies. *Id.* at 963. Writing separately, Justice Sotomayor agreed and explained that "GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *Id.* at 956.

The Supreme Court has also made clear that location tracking that reveals otherwise undiscoverable facts about protected spaces implicates the Fourth Amendment. In *United States v. Karo*, 468 U.S. 705 (1984), the Court held that location tracking implicates Fourth Amendment privacy interests because it may reveal information about individuals in areas where they have reasonable expectations of privacy. The Court explained that using an electronic device—there, a beeper—to infer facts about "location[s] not open to visual surveillance," like whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises, was just as unreasonable as searching the location without a warrant. *Id*. at 714–15. Such location tracking, the Court ruled, "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through

visual surveillance" from a public place, *id*. at 707, regardless of whether it reveals that information directly or through inference. *See also Kyllo v. United States*, 533 U.S. 27, 36 (2001) (rejecting "the novel proposition that inference insulates a search," noting that it was "blatantly contrary" to the Court's holding in *Karo* "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home").

If tracking a car's location for 28 days violates an expectation of privacy that society is prepared to recognize as reasonable, then surely tracking a cell phone's location for 67 days does as well. Just as "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," *Jones*, 132 S. Ct. at 964 (Alito, J.), so, too, is it society's expectation that government agents would not track the location of a cell phone for 67 days. The expectation that a cell phone will not be tracked is even more acute than is the expectation that cars will not be tracked because individuals are only in their cars for discrete periods of time, but carry their cell phones with them wherever they go, including inside Fourth-Amendment-protected private spaces. Moreover, cars are visible on the public street, whereas individuals generally keep their cell phones in a concealed place when not actively in use. *See United States v. Powell*, __ F. Supp. 2d __, 2013 WL 1876761, at *13 (E.D. Mich. May 3, 2013) ("There are practical limits on where a

GPS tracking device attached a person's vehicle may go. A cell phone, on the other hand, is usually carried with a person *wherever* they go.").

Although at the suppression hearing the government pointed out that *Jones* addressed real-time location tracking while this case involves historical location data, D.E. 277, at 12, 35, that is a distinction without a difference. "The temporal distinction between prospective and historical location tracking is not compelling, because the degree of invasiveness is the same, whether the tracking covers the previous 60 days or the next. . . . 'The picture of [a person's] life the government seeks to obtain is no less intimate simply because it has already been painted.'" *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 839 (S.D. Tex. 2010), *argued*, No. 11–20884 (5th Cir. Oct. 2, 2012). Because there is no meaningful distinction between the information the government seeks in this case and the information the government sought in *Jones*, the government's actions constituted a search.

Further, cell phone location data implicates Fourth Amendment interests because, like the tracking in *Karo*, it reveals or enables the government to infer information about whether the cell phone is inside a protected location and whether it remains there. The cell phone travels through many such protected locations during the day where, under *Karo*, the government cannot warrantlessly intrude on individuals' reasonable expectations of privacy. *See, e.g. Kyllo*, 533 U.S. at 31

(home); *See v. City of Seattle*, 387 U.S. 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483, 486-88 (1964) (hotel room). "If at any point a tracked cell phone signaled that it was inside a private residence (or other location protected by the Fourth Amendment), the only other way for the government to have obtained that information would be by entry into the protected area, which the government could not do without a warrant." *Powell*, 2013 WL 1876761, at *11.

This is true even if cell phone location data is less precise than GPS data, because even imprecise information, when combined with visual surveillance or a known address, can enable law enforcement to infer the exact location of a phone. *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 311 (3d Cir. 2010) ["Third Circuit Opinion"] Indeed, that is exactly how the government's experts routinely use such data; "the Government has asserted in other cases that a jury should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home." *Id.* at 311–12. In this case, the police officer who analyzed Defendant's cell phone location data testified during the prosecution's case in chief that he was able to determine which cell site was nearest to Defendant's home, and to draw conclusions about when he was and was not at home from the CSLI. D.E. 285, at 42, 49–51. And indeed, Defendant's cell phone records frequently indicate when he was home. *Supra* Part I.A.ii. Moreover, the

rapid proliferation of femtocells means that for many people, cell site location records will reveal their location to the accuracy of a floor or room within their home. When the government requests historical cell site information it has no way to know in advance how many cell site data points will be for femtocells or geographically small sectors of conventional cell towers, or will otherwise reveal information about a Fourth-Amendment-protected location. As the Court observed in *Kyllo*, "[n]o police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." 533 U.S. at 39; *accord Powell*, 2013 WL 1876761, at *12 (applying *Kyllo* to cell site location information). A warrant is therefore required.

Moreover, the government's own use of the records in this case belies its argument that they are imprecise. Although in opposing the motion to suppress the government asserted that CSLI is "not precise," D.E. 277, at 13, at trial the prosecution used Defendant's CSLI to demonstrate, among other things, that Defendant was "literally right up against the Amerika Gas Station immediately preceding and after that robbery occurred," D.E. 285, at 58, that he was "literally . . . right next door to the Walgreen's just before and just after that store was robbed," *id.* at 61, and that Defendant and his alleged co-conspirators were "literally right on top of the Advance Auto Parts one minute before that robbery

took place, D.E. 287, at 13. The government relied on Defendant's CSLI to show where he was, who he was with, and what he was doing. *See* Ex. C; D.E. 285, at 23–38, 55–56, 58, 61, 64–65, 66; D.E. 287, at 4–5, 12–15, 23, 63–66. Law enforcement combed through two months of Defendant's location records without a warrant. When the government found 39 of Defendant's location data points that it believed corroborated its theory of the case, Ex. C, it asserted their accuracy and probativeness to the jury. *See, e.g.*, D.E. 285, at 23–35. But the government incredibly insists that all 11,567 remaining data points reveal nothing private about Defendant's life. D.E. 277, at 13, 35. Quite the opposite: long-term data about Defendant's locations and movements reveals much information that society recognizes as justifiably private, and its warrantless acquisition violates the Fourth Amendment. The district court erred in discounting the view of five members of the Supreme Court that longer term location tracking obtained by electronic means is a Fourth Amendment search.

C. Cell Phone Providers' Ability to Access Customers' Location Data Does Not Eliminate Cell Phone Users' Reasonable Expectation of Privacy in That Data.

The government argued that Defendant has no reasonable expectation of privacy in his cell phone location information because, under Supreme Court precedent, that information was conveyed to MetroPCS and was contained in MetroPCS's business records. D.E. 277, at 35–37. On the contrary, Defendant

never voluntarily conveyed his location information to his wireless carrier, and the Court's business records cases do not extend to the scenario presented here. Moreover, the only circuit to address the issue to date has rejected the government's position, holding that cell phone users may maintain a reasonable expectation of privacy in their location records even though these records are held by a third party business. *Third Circuit Opinion*, 620 F.3d at 317–18. That is the correct conclusion, and this Court should follow it here.

The Supreme Court cases on which the government apparently relies do not reach the government surveillance at issue in this case. In *United States v. Miller*, 425 U.S. 435 (1976), the Court held that a bank depositor had no expectation of privacy in records about his transactions that were held by the bank. Although the Court explained that the records were the bank's business records, *id.* at 440, it proceeded to inquire whether Miller could nonetheless maintain a reasonable expectation of privacy in the records: "We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Id.* at 442. The Court's ultimate conclusion—that Miller had no such expectation—turned not on the fact that the records were owned or possessed by the bank, but on the fact that Miller "voluntarily conveyed" the information contained in them to the bank and its employees. *Id.*

In *Smith v. Maryland*, 442 U.S. 735 (1979), the Court held that the use of a pen register to capture the telephone numbers an individual dials was not a search under the Fourth Amendment. *Id.* at 739, 742. The Court relied heavily on the fact that when dialing a phone number the caller "voluntarily convey[s] numerical information to the telephone company." *Id.* at 744. As in *Miller*, in addition to establishing voluntary conveyance the Court also assessed the degree of invasiveness of the surveillance at issue to determine whether the user had a reasonable expectation of privacy. The Court noted the "pen register's limited capabilities," *id.* at 742, explaining that "'a law enforcement official could not even determine from the use of a pen register whether a communication existed.'" *Id.* at 741 (quoting *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 167 (1977)).

Assessing an individual's expectation of privacy in cell phone location information thus turns on whether the contents of the location records were voluntarily conveyed to the wireless provider, and what privacy interest the person retains in the records. The Third Circuit has explained why cell phone users retain a reasonable expectation of privacy in their location information:

> A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone 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 cell phone user receives a call, he hasn't voluntarily exposed anything at all."

Third Circuit Opinion, 620 F.3d at 318–19 (last alteration in original).

There is nothing inherent in placing a cell phone call that would indicate to callers that they are exposing their location information to their wireless carrier. In both *Miller* and *Smith*, the relevant documents and dialed numbers were directly and voluntarily conveyed to bank tellers and telephone operators, or their automated equivalents. *See, e.g.*, *Smith*, 442 U.S. at 744. But when a cell phone user makes or receives a call, there is no indication that making or receiving the call will also create a record of the caller's location. The user does not input her location information into the phone, and the phone does not notify the user that her location has been logged. Moreover, unlike the dialed phone numbers at issue in *Smith*, location information does not appear on a typical user's monthly bill. *See id.* at 742. Further, many smartphones include a location privacy setting that, when enabled, prevents applications from accessing the phone's location. However, this setting has no impact at all upon carriers' ability to learn the cell sector in use, thus potentially misleading phone users. Cell site location information is automatically determined by the wireless provider, but is not actively, intentionally, or affirmatively disclosed by the caller.

The government acknowledged as much at trial. During the prosecution's case in chief, MetroPCS's custodian of records testified that "the caller and

receiver, they never know what is going on" when calls are routed between cell towers. D.E. 283, at 223. At the start of its closing argument, the prosecution explained that "what this defendant could not have known was that . . . his cell phone was tracking his every moment." D.E. 287, at 4–5. And later in the prosecution's closing, counsel for the government stated that Defendant and his alleged co-conspirators "had no idea that by bringing their cell phones with them to these robberies they were allowing MetroPCS . . . to follow their movements." *Id.* at 14.

Further, the existence of MetroPCS's privacy policy on its website does nothing to convert automatic, involuntary retention of location information into voluntary conveyance of such data. The version of the privacy policy in effect when the government requested Defendant's location records provided limited discussion of the location data automatically stored by MetroPCS, but did not specify a length of time the information was retained. Privacy Policy, MetroPCS (archived Mar. 4, 2010).[30] The government made no showing that Defendant was actually aware that MetroPCS's privacy policy existed, much less that he read or understood it. *Cf.* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1032 & n.34 (2012) (noting that most

[30] *Available at* http://web.archive.org/web/20100304225035/http://www.metropcs.com/privacy/privacy.aspx.

consumers do not read privacy policies). Even if he was aware of its existence, it is likely that Defendant would have thought the privacy policy would *protect against* collection and disclosure of information, not facilitate it.[31] Indeed, the privacy policy misleadingly stated that "[u]nder federal law, you have a right, and we have a duty, to protect the confidentiality of information about . . . the location of your device on our network when you make a voice call." Privacy Policy, *supra*.

Moreover, the fact that cell phone location information is handled by a third party is not dispositive. The Sixth Circuit's opinion in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), is instructive. There, the court held that there is a reasonable expectation of privacy in the contents of emails. The court explained that the fact that email is sent through an internet service provider's servers does not vitiate the legitimate interest in email privacy: both letters and phone calls are sent via third parties (the postal service and phone companies), but people retain a reasonable expectation of privacy in those forms of communication. *Id.* at 285 (citing *Katz*, 389 U.S. at 353; *United States v. Jacobsen*, 466 U.S. 109, 114 (1984)). *Warshak* further held that even if a company has a right to access information in certain circumstances under the terms of service (such as to scan

[31] *See* Joseph Turrow et al., *Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace* 1 (2007), *available at* http://www.law.berkeley.edu/files/annenberg_samuelson_advertising.pdf (reporting that most people think the mere existence of a privacy policy on a website means "the site will not share my information with other websites or companies").

emails for viruses or spam), that does not necessarily eliminate the customer's reasonable expectation of privacy vis-à-vis the government. *Id.* at 286–88. In a variety of contexts under the Fourth Amendment, access to a protected area for one limited purpose does not render that area suddenly unprotected from government searches. *See, e.g.*, *United States v. Washington*, 573 F.3d 279, 284 (6th Cir. 2009) (tenants have reasonable expectation of privacy in their apartments even though landlords have a right to enter); *United States v. Paige*, 136 F.3d 1012, 1020 n.11 (5th Cir. 1998) ("[A] homeowner's legitimate and significant privacy expectation . . . cannot be entirely frustrated simply because, *ipso facto*, a private party (*e.g.*, an exterminator, a carpet cleaner, or a roofer) views some of these possessions."); *United States v. Brazel*, 102 F.3d 1120, 1148 (11th Cir. 1997) ("[A] landlord generally lacks common authority to consent to a search of a tenant's apartment . . . ." (citing *Chapman v. United States*, 365 U.S. 610 (1961))).

Like the contents of emails, cell phone location information is not a simple business record voluntarily conveyed by the customer. In this case the government obtained a transcript of four individuals' locations and movements over a staggering 67 days. D.E. 266. The Supreme Court has cautioned that new technologies should not be allowed to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34; *see also Warshak*, 631 F.3d at 285 ("[T]he Fourth Amendment must keep pace with the inexorable march of technological

progress, or its guarantees will wither and perish."). If this Court holds that cell phone tracking falls outside of the ambit of the Fourth Amendment, the Supreme Court's decision in *Jones* will have little practical effect in safeguarding Americans from the pervasive monitoring of their movements that so troubled a majority of the Justices. *See Jones*, 132 S. Ct. at 955 (Sotomayor, J.); *id.* at 963–64 (Alito, J.).

II. EVEN IF THE GOOD FAITH EXCEPTION APPLIES, THIS COURT SHOULD DECIDE THE FOURTH AMENDMENT QUESTION.

This Court should decide that a search of long-term historical CSLI requires a probable cause warrant regardless of whether the good faith exception applies. When a case presents a "novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates, there is sufficient reason for the Court to decide the violation issue *before* turning to the good-faith question." *Illinois v. Gates*, 462 U.S. 213, 264, 265 n.18 (1983) (White, J., concurring) (citing *O'Connor v. Donaldson*, 422 U.S. 563 (1975) (finding a constitutional violation and remanding for consideration of the good faith defense)). This is just such a case. Cell site location tracking has become a favored tool of law enforcement and is already used far more frequently than the GPS tracking technology in *Jones*. Its highly intrusive nature cries out for clear judicial regulation.

In *Warshak*, the Sixth Circuit explained the importance of addressing important Fourth Amendment issues even when the good faith exception will ultimately apply:

> Though we may surely do so, we decline to limit our inquiry to the issue of good faith reliance. If every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the government would be given *carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a statute supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations. In other words, if the exclusionary rule is to have any bite, courts must, from time to time, decide whether statutorily sanctioned conduct oversteps constitutional boundaries.

631 F.3d at 282 n.13 (citation omitted). The Sixth Circuit's logic is not novel: courts frequently decide whether there has been a Fourth Amendment violation before applying the good faith exception. For example, this Court recently decided that the search of a vehicle violated the Fourth Amendment pursuant to *Arizona v. Gant*, 556 U.S. 332 (2009), and only then applied the good faith exception to the exclusionary rule. *United States v. Davis*, 598 F.3d 1259, 1263–68 (11th Cir. 2010), *aff'd* 131 S. Ct. 2419 (2011). Similarly, when assessing whether search warrants satisfy the Fourth Amendment's probable cause and particularity requirements, courts frequently find a Fourth Amendment violation *before* turning to the good faith doctrine. *See, e.g.*, *United States v. Burrell*, 445 F. App'x 195, 197 (11th Cir. 2011) (per curiam); *United States v. Clark*, 638 F.3d 89, 91 (2d Cir. 2011); *United States v. Otero*, 563 F.3d 1127, 1131–1133 (10th Cir. 2009). This

approach is no less appropriate in the location tracking context. *See Powell*, 2013 WL 1876761, at *11–20 (holding that government lacked probable cause to engage in cell phone location tracking, and then applying good faith exception); *United States v. Ford*, No. 1:11–CR–42, 2012 WL 5366049, at *7–11 (E.D. Tenn. Oct. 30, 2012) (determining that warrantless GPS tracking violates the Fourth Amendment, and then applying good faith exception).

Phone companies have been inundated with law enforcement requests for location data in recent years: from 2007 to 2012, for example, Sprint/Nextel received nearly 200,000 court orders for cell phone location information.[32] From 2006 to 2012, MetroPCS, Defendant's carrier, "responded to an average of fewer than 12,000 requests per month from law enforcement to provide information about MetroPCS' customers' phone usage."[33] As the use of cell phones becomes ubiquitous and cell site location information becomes ever-more precise, it is crucial for courts to provide guidance to law enforcement and the public about the

[32] Letter from Vonya B. McCann, Senior Vice President, Sprint, to Rep. Edward J. Markey (May 23, 2012), a*vailable at* http://web.archive.org/web/20130415200646/http://markey.house.gov/sites/markey.house.gov/files/documents/Sprint%20Response%20to%20Rep.%20Markey.pdf.

[33] Letter from Steve Cochran, Vice President, MetroPCS Commc'ns, Inc., to Rep. Edward J. Markey 1 (May 23, 2012), *available at* http://web.archive.org/web/20130318011325/http://markey.house.gov/sites/markey.house.gov/files/documents/MetroPCS%20Response%20to%20Rep.%20Markey.PDF. This figure is not limited to requests for cell phone location information only.

scope of the Fourth Amendment. The issue is now before this Court, and addressing it would yield much needed clarity in this Circuit.

CONCLUSION

Because the collection of long-term cell phone location information violates reasonable expectations of privacy, this Court should hold that a warrant is required for such searches under the Fourth Amendment.

Respectfully Submitted,

Dated: July 17, 2013

By: /s/ Maria Kayanan
Maria Kayanan
mkayanan@aclufl.org
Fla. Bar No. 305601
ACLU Foundation of Florida, Inc.
4500 Biscayne Blvd. Ste. 340
Miami, FL 33137
Tel: 786-363-2700
Fax: 786-363-3108

Nathan Freed Wessler (*admission pending*)
nwessler@aclu.org
Catherine Crump
Ben Wizner
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel: 212-549-2500
Fax: 212-549-2654

Benjamin James Stevenson
bstevenson@aclufl.org
Fla. Bar No. 589909
ACLU Foundation of Florida, Inc.

P.O. Box 12723
Pensacola, FL 32591-2723
Tel: 786-363-2738
Fax: 786-363-1985

Kevin S. Bankston
Gregory T. Nojeim
Center for Democracy & Technology
1634 I St NW, Suite 1100
Washington, DC 20006
(202) 637-9800

Hanni Fakhoury
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

David Oscar Markus
Vice-Chair, 11th Circuit Amicus Committee
Nat'l Ass'n of Criminal Defense Lawyers
Markus & Markus, PLLC
40 N.W. 3rd Street,
Penthouse One
Miami, Florida 33128
Telephone No. (305) 379-6667
Facsimile No. (305) 379-6668
dmarkus@markuslaw.com

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a) because it contains 6,980 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).
2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman.

/s/ Maria Kayanan

Maria Kayanan

July 17, 2013

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 17th day of July, 2013, the foregoing Amici Curiae Brief for the American Civil Liberties Union Foundation, American Civil Liberties Union Foundation of Florida, Center for Democracy & Technology, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system.

/s/ Maria Kayanan

Maria Kayanan