

STATE OF NEW JERSEY,
Plaintiff

v.

Thomas W. EARLS,
Defendant

| SUPREME COURT OF NEW JERSEY
| DOCKET NO. 68,765
| Appeal No. A-53-11
|

| Criminal Action
|

| On Appeal from a Final Order
| of the Superior Court,
| Appellate Division, Affirming
| the Judgment of Conviction
|

| Sat Below:

| Hon. Anthony J. Parrillo, JAD
| Hon. Patricia B. Roe, JAD
| Hon. Stephen Skillman, JAD

**SUPPLEMENTAL BRIEF OF *AMICUS CURIAE*
ELECTRONIC PRIVACY INFORMATION CENTER**

On the brief:
Grayson Barber
Marc Rotenberg
Alan Butler

GRAYSON BARBER
Grayson Barber, LLC
68 Locust Lane
Princeton, NJ 08540
(609) 921-0391
*Counsel of Record for
Proposed Amicus Curiae
Electronic Privacy
Information Center*

MARC ROTENBERG
Electronic Privacy
Information Center
1718 Connecticut Ave NW
Suite 200
Washington, DC 20009
(202) 483-1140

TABLE OF CONTENTS

Table of Contents **i**

Table of Authorities **ii**

PRELIMINARY STATEMENT **1**

ARGUMENT **2**

 I. Current Technology Allows Law Enforcement to Pinpoint the Location of Mobile Devices, Even in a Private Residence, Using a Variety of Methods..... 3

 A. Mobile Devices Include Cell Phones, Smartphones, and Other Wireless Data-Enabled Devices 3

 B. Current Technologies Can Precisely Locate a Device Using Network-based, Handset-based, or Third Party Methods 8

 II. Reasonable Expectation of Privacy in Location of Modern Cell Phones Under Federal and State Constitutions..... 17

 A. Individuals Have a Reasonable Expectation of Privacy in the Location of Their Modern Cell Phones Under the Federal Constitution 18

 B. An Individual's Reasonable Expectation of Privacy in the Location of Their Cell Phone Is Not Eliminated by the Third Party Doctrine Because Location Data Is Not Voluntarily Disclosed and It Is Protected Under the Communications Act 27

 C. Many State Supreme Courts Provide Privacy Protections at Least as Expansive as the Fourth Amendment, and New Jersey and Other States Explicitly Recognize Privacy Rights in Records Held by Third Parties 28

CONCLUSION **30**

TABLE OF AUTHORITIES

CASES

Commonwealth v. Connolly, 454 Mass. 808 (2009)29

Commonwealth v. Wyatt, 30 Mass.L.Rptr. 270 (Mass. Sup. Ct. 2012)21, 29

In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005) 24

In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 384 F. Supp. 2d 562 (E.D.N.Y. 2005) .. 24

In re Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register, 415 F. Supp. 2d 211 (W.D.N.Y. 2006) 24

In re Application of the U.S. for an Order Authorizing the Use of a Pen Register and Trap and Trace Device, ___ F. Supp. 2d ___, 2012 WL 2120492 (S.D. Tex. 2012) 17

In re Application of U.S. for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed], 402 F. Supp. 2d 597 (D. Md. 2005)21, 24, 25

In re Application of U.S. for an Order Directing a Provider of Electronic Communications Service to Disclose Records to Government, 620 F.3d 304 (3d Cir. 2010)21, 25, 27

In re Application, 439 F. Supp. 2d 456 (D. Md. 2006) 24

In re The Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 132 (D.D.C. 2005) 24

In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d), Nos. 12-670, 671, 672, 673, 674, 2012 WL 4717778 (S.D. Tex. Sept. 26, 2012) 13

In re U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947 (E.D. Wisc. 2006) 24

In re U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010) 21

In re U.S. for Orders Authorizing Installation and Use of Pen Registers, 416 F. Supp. 2d 390 (D. Md. 2006) 24

In re U.S., 441 F. Supp. 2d 816 (S.D.N.Y. 2006) 24

<i>In re U.S., Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847 (N.D. Ind. July 5, 2006)</i>	24
<i>Karo v. United States</i> , 468 <u>U.S.</u> 705 (1984)	20, 23
<i>Katz v. United States</i> , 389 <u>U.S.</u> 347 (1967)	19
<i>Kyllo v. United States</i> , 533 <u>U.S.</u> 27, 32-33 (2001)	18, 19
<i>People v. Hall</i> , 86 <u>A.D.3d</u> 450 (N.Y. App. Div. 1st 2011)	29
<i>People v. Oates</i> , 698 <u>P.2d</u> 811 (Colo. 1986)	29
<i>People v. Weaver</i> , 12 <u>N.Y.3d</u> 433 (2009)	21, 22, 29
<i>Smith v. Maryland</i> , 442 <u>U.S.</u> 735 (1979)	18, 27
<i>State v. Holden</i> , 54 <u>A.3d</u> 1123 (Del. Super. Ct. 2010)	21
<i>State v. Jackson</i> , 150 <u>Wash.2d</u> 251 (2003)	21
<i>State v. Zahn</i> , 812 <u>N.W.2d</u> 490 (S.C. 2012)	21
<i>United States v. Forest</i> , 355 <u>F.3d</u> 942 (6th Cir. 2004), <i>vacated and remanded on other grounds sub nom. Garner v. United States</i> , 542 <u>U.S.</u> 1100 (2005)	27
<i>United States v. Jones</i> , 132 <u>S. Ct.</u> 945 (2012)	2, 20, 21, 26
<i>United States v. Jones</i> , 132 <u>S. Ct.</u> 945 (2012) (Alito, J., concurring)	21
<i>United States v. Jones</i> , 132 <u>S. Ct.</u> 945 (2012) (Sotomayor, J., concurring)	21
<i>United States v. Knotts</i> , 460 <u>U.S.</u> 276 (1983)	20
<i>United States v. Miller</i> , 425 <u>U.S.</u> 435 (1976)	18, 27
<i>United States v. Williams</i> , 650 <u>F. Supp. 2d</u> 633 (W.D. Ky. 2009)	21

STATUTES

18 U.S.C. § 2510(12) (D)	24
18 U.S.C. § 2703(d)	25
18 U.S.C. § 3117	24
18 U.S.C. § 3121 <i>et seq.</i>	25
47 U.S.C. § 1002(a)	23
47 U.S.C. § 222	9
47 U.S.C. § 222(d) (4)	9, 28
47 U.S.C. § 222(f)	28
Communications Assistance for Law Enforcement Act ("CALEA") in 1994, Pub. L. 103-414, 108 Stat. 4280	23
Wireless Communications and Public Safety Act of 1999, Pub. L. 106-81, 113 Stat. 1286 (1999)	27

REGULATIONS

47 C.F.R. § 20.18 9
47 C.F.R. § 20.18(h) 9

ADMINISTRATIVE & LEGISLATIVE MATERIALS

Fed. Commc'ns Comm'n, Fifteenth Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial Mobile Radio Services (2011) .. 5
U.S. Dep't of Health & Human Servs., Ctrs. for Disease Control & Prevention, Nat'l Center for Health Statistics, Wireless Substitution: State-level Estimates from the National Health Interview Survey, 2010-2011, 61 Nat'l Health Stat. Rep. 1 (Oct. 12, 2012) 5

OTHER AUTHORITIES

A Guide to the Wireless Engineering Body of Knowledge 77 (Andrzej Jajszczyk ed., 2nd ed. 2011) 10
Aaron Smith, The Best (and Worst) of Mobile Connectivity, Pew Internet & American Life Project (Nov. 30, 2012) 23
Adam Gorski, Understanding GPS Performance in Urban Environments, AGI (Jan. 4, 2011) 15
Ali H. Sayed, Alireza Tarighat & Nima Khajehnouri, Network-Based Wireless Location, IEEE Signal Processing Magazine 24 (Jul. 2005) 10, 13
America's New Mobile Majority: a Look at Smartphone Owners in the U.S., Nielsen Wire (May 7, 2012) 7
Ann Cavoukian & Kim Cameron, Wi-Fi Positioning Systems: Beware of Unintended Consequences (June 2011) 15, 16
Apple, iPad with Wi-Fi + Cellular (2012) 8
Apple, iPhone: Built-in Apps (2012) 7
Ariane de Vogue, Supreme Court Ruling Prompts FBI to Turn Off 3,000 Tracking Devices, Yahoo! News (Mar. 7, 2012) 22
Axel Küpper, Location-Based Services: Fundamentals and Operation (2006) 4, 10, 12, 13, 14, 15
Brian Fling, Mobile Design and Development (2009) 7
CDG, Welcome to the World of CDMA: Glossary 4, 10, 11
CTIA: The Wireless Ass'n, Wireless in America: Wireless Subscriber Statistics (May 2011) 12
CTIA: The Wireless Association, Wireless in America: How Wireless Works (Jan. 2011) 4, 10
CTIA: The Wireless Association, Wireless Quick Facts (2012) 5

Dimitris Mavrikis, <u>Do We Really Need Femto Cells?</u> , <i>Vision Mobile</i> (Dec. 1, 2007)	12
Don Kellogg, <u>40 Percent of U.S. Mobile Users Own Smartphones; 40 Percent are Android</u> , <i>Nielsen Wire</i> (Sept. 1, 2011)	6
<i>Fed. Commc'ns Comm'n</i> , <u>Enhanced 9-1-1 - Wireless Services</u>	9
Frank Van Diggelen, <u>A-GPS: Assisted GPS, GNSS, and SBAS</u> (2009)	14
Google, <u>Statement to Several National Data Protection Authorities</u> (Apr. 27, 2010)	16
Heather Kelly, <u>OMG, the Text Message Turns 20. But Has SMS Peaked?</u> , <i>CNN</i> (Dec. 3, 2012)	6
Janice Y. Tsai et al., <u>Location-Sharing Technologies: Privacy Risks and Controls</u> (2010)	26
Jennifer Valentino-Devries, <u>Stingray Phone Tracker Fuels Constitutional Clash</u> , <i>Wall St. J.</i> , Sept. 22, 2011	16
John R. Quain, <u>Changes to OnStar's Privacy Terms Rile Some Users</u> , <i>N.Y. Times Blog: Wheels</i> (Sept. 22, 2011)	26
Junhui Zhao & Xueue Zhang, <u>Location-Based Services Handbook: Wireless Location Technology in Location-Based Services</u> (Syed A. Ahson & Mohammad Ilyas eds., 2011)	12
<u>Kindle Fire HD 8.9: Faster Processor, Larger Screen, and 4G Coming Soon</u> , <i>CNET</i> (Sept. 23, 2012)	8
M. Wesley Clark, <u>Cell Phones as Tracking Devices</u> , 41 <i>Val. U. L. Rev.</i> 1413 (2007)	20
Maeve Duggan & Lee Rainie, <u>Cell Phone Activities 2012</u> , <i>Pew Internet & American Life Project</i> (Nov. 25, 2012)	7
Mail2Web, <u>Mobile Email from mail2web.com Keeps You Connected</u> (2012)	8
Michael Benisch et al., <u>Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs</u> , 15 <i>Personal & Ubiquitous Comp.</i> 679 (2011)	26
Michele Sequeira & Michael Westphal, <u>Cell Phone Science: What Happens When You Call and Why</u> (2010)	10
Nick Bilton, <u>Tracking File Found in iPhones</u> , <i>N.Y. Times</i> , Apr. 20, 2011	26
Nicole Lee, <u>The 411: Feature Phones v. Smartphones</u> , <i>CNET</i> (Mar. 1, 2010)	7
Nishith D. Tripathi, Jeffrey H. Reed & Hugh F. VanLandingham, <u>Handoff in Cellular Systems</u> , <i>IEEE Pers. Comm.</i> , Dec. 1998	11

Orin Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311 (2012)21

Press Release, Small Cells Outnumber Traditional Mobile Base Stations, Small Cell Forum (Oct. 31, 2012)12

Samsung, Galaxy Tab 10.1 Feature 8

Stephanie K. Pell & Christopher Soghoian, Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact, 26 Berkeley Tech. L.J. 117 (2012) 11

Stephen E. Henderson, Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search, 55 Cath. U. L. Rev. 373 (2007)28, 29

Susan Freiwald, Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact, 70 Md. L. Rev. 681 (2011) 11

Tom Farley & Mark van der Hoek, Cellular Telephone Basics (Jan. 1, 2006) 4

U.S. Air Force, Global Positioning System Factsheet (Sept. 15, 2010)14

Verizon Wireless, Wireless Issues: Enhanced 911 (2012) 6

PRELIMINARY STATEMENT

On November 21, 2012 this Court requested additional briefing from all parties to address six specific questions of law and fact relevant to the cell phone location tracking issue in this case. Given EPIC's role as *amicus curiae*¹ in this case and its expertise in legal and technological issues related to privacy and civil liberties, this supplemental *amicus* brief will address questions 5 and 6 presented by the court:

5) Please describe the current state of technology relating to cell phone location tracking and similar technologies.

6) Do cell phone users today have a reasonable expectation of privacy in the location of modern cell phones under the federal and state constitutions?

This case implicates a key privacy issue for all cell phone users: the application of federal and state constitutional privacy protections to location records collected from modern cell phones. These location records can be used to identify activities, movements, and relationships that would otherwise be private because they take place in protected spaces. Cell phones have become ubiquitous, and are an essential tool in the everyday lives of most Americans. As such, the consequence of an adverse determination regarding the privacy issue before this Court would be substantial.

¹ This brief was prepared with the assistance of Jeramie D. Scott, EPIC's National Security Fellow.

ARGUMENT

Modern cell phones permit the government to collect far more detailed personal information than it was able to gather in the past. Current technology enables law enforcement to locate individuals within buildings and even within particular rooms by collecting location data from their cell phones. The data can either be collected directly using surveillance technology or indirectly through the service provider. In most cases, an individual's only means of avoiding such tracking is by physically powering off their mobile device and removing the battery. The simple act of making a phone call, sending a text message, checking a web page, or even automatically syncing e-mail can enable tracking of a user's exact location within the home or other private location. None of these actions necessarily require the collection or disclosure of a user's location. In some circumstances, the location of a cell phone may be tracked without the user taking any affirmative action.

Given the current state of technology, collection and use of location data from modern cell phones clearly implicates an individual's reasonable expectation of privacy. The Supreme Court's recent decision in United States v. Jones, 132 S. Ct. 945 (2012), indicates the Court's refusal to allow broad location surveillance without careful review under the Fourth Amendment. The standards that applied to infrequent, low-tech

radio tracking are unworkable in the context of ubiquitous location data. Federal and state courts are still in the process of adapting as technology changes, but the need for privacy safeguards is clear.

I. Current Technology Allows Law Enforcement to Pinpoint the Location of Mobile Devices, Even in a Private Residence, Using a Variety of Methods

Cell phones, smartphones, and other mobile devices (e.g. laptops and tablets) can be located whenever they are turned on. Current location-tracking technologies can be used to pinpoint users of mobile devices in several ways. First, service providers have access to network-based and handset-based technologies that can locate a phone for emergency purposes. Second, historical location can frequently be discerned from service provider records. Finally, third party devices such as Wi-Fi hotspots or IMSI catchers can be used to track nearby mobile devices in real time. The accuracy of these methods depends on a variety of technological and environmental factors, but the location data will only get more precise as the technology evolves.

A. Mobile Devices Include Cell Phones, Smartphones, and Other Wireless Data-Enabled Devices

Mobile devices that are currently used and identified by location tracking technologies fall into three categories: cell phones, smartphones, and other wireless data-enabled devices.

A cell phone is "a very sophisticated and versatile" device that uses radio waves to send and receive voice calls and data whenever it is within range of an antenna or tower. CTIA: The Wireless Association, Wireless in America: How Wireless Works (Jan. 2011).² Cell phones connect to a service provider's network via "cell sites" that contain a transceiver and controller used to relay signals to and from mobile devices to the network switch. Axel Küpper, Location-Based Services: Fundamentals and Operation 91-92 (2006).³ The cell sites provide a link to the network's mobile telecommunications switching office, which facilitates calls and other communications to and from mobile devices. Id. at 93-97.

According to the most recent federal wireless competition report, there were an estimated 290.7 million connected wireless devices in the United States in 2009. Fed. Commc'ns Comm'n, Fifteenth Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial

² Available at

http://files.ctia.org/pdf/WirelessInAmerica_Jan2011.pdf.

³ See generally CDG, Welcome to the World of CDMA: Glossary, http://www.cdg.org/technology/cdma_technology/a_ross/DefAtoF.asp (last accessed Dec. 20, 2012) [hereinafter CDMA Glossary]; Tom Farley & Mark van der Hoek, Cellular Telephone Basics (Jan. 1, 2006), http://www.privateline.com/mt_cellbasics/i_introduction/ (useful descriptions of cell phone concepts on a site moderated by telecommunications experts).

Mobile Radio Services 97 (2011).⁴ Based on those figures, the FCC estimates that roughly 94 out of every 100 Americans own a cell phone. Id. at 95-96. Another recent government report found that in 2011 one in three U.S. households had only wireless telephones. U.S. Dep't of Health & Human Servs., Ctrs. for Disease Control & Prevention, Nat'l Center for Health Statistics, Wireless Substitution: State-level Estimates from the National Health Interview Survey, 2010-2011, 61 Nat'l Health Stat. Rep. 1 (Oct. 12, 2012).⁵ By contrast, just 10% of households had only landline phones. Id.

Many modern cell phones also contain GPS chips, which can be used to facilitate emergency 911 ("E-911") services even when the device itself has no mapping or other location-based functionality. For example, "100% of the new handsets sold by Verizon Wireless since December 31, 2003 are GPS-capable, which means there is a chipset in the phone that will help provide location information." Verizon Wireless, Wireless Issues:

⁴ Available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-11-103A1.pdf. According to CTIA: The Wireless Association, there were 321.7 million subscriber connections as of Jun 2012. CTIA: The Wireless Association, Wireless Quick Facts (2012), <http://www.ctia.org/advocacy/research/index.cfm/aid/10323>. That means there are currently more mobile devices in the United States than people. Id.

⁵ Available at <http://www.cdc.gov/nchs/data/nhsr/nhsr061.pdf>

Enhanced 911 (2012).⁶ However, some wireless carriers represent that this location tracking can only function “when the network is prompted to determine the mobile’s location” after dialing 911. Verizon Wireless, E911 Compliance FAQs (2012).⁷ Most non-smartphone users likely do not know that their device contains GPS technology that can be used to locate them.

Current mobile technology makes it increasingly easy to locate users. For twenty years, basic cell phones have been capable of sending and receiving text messages. See Heather Kelly, OMG, the Text Message Turns 20. But Has SMS Peaked?, CNN (Dec. 3, 2012).⁸ The majority of cell phones sold today are actually “feature phones” that have additional pre-programmed features. Don Kellogg, 40 Percent of U.S. Mobile Users Own Smartphones; 40 Percent are Android, Nielsen Wire (Sept. 1, 2011).⁹ They are “a midway point between smartphones and basic phones.” Nicole Lee, The 411: Feature Phones v. Smartphones,

⁶

<http://aboutus.verizonwireless.com/wirelessissues/enhanced911.html>.

⁷

http://support.verizonwireless.com/faqs/Wireless%20Issues/faq_e911_compliance.html.

⁸ <http://edition.cnn.com/2012/12/03/tech/mobile/sms-text-message-20/>.

⁹ http://blog.nielsen.com/nielsenwire/online_mobile/40-percent-of-u-s-mobile-users-own-smartphones-40-percent-are-android/.

CNET (Mar. 1, 2010).¹⁰ Feature phones are capable of many things the user may not even realize, such as generating location data.

It is not always easy to distinguish between a smartphone and a feature phone, but current smartphones typically have an advanced operating system, a large screen, a keyboard or other input device, and high-speed data connection such as Wi-Fi. Brian Fling, Mobile Design and Development (2009). According to a 2012 Nielsen survey, a "majority (50.4%) of U.S. mobile subscribers owned smartphones." America's New Mobile Majority: a Look at Smartphone Owners in the U.S., Nielsen Wire (May 7, 2012).¹¹ The critical difference between smartphones and others for location tracking purposes is that smartphone users can connect to the Internet and sync their e-mail with their phones. See, e.g., Apple, iPhone: Built-in Apps (2012).¹² These repeated connections create countless cell site records.

A recent Pew survey found that 50% of cell phone owners use their phones to send and receive e-mail, and more than 50% access the internet on their phones. Maeve Duggan & Lee Rainie, Cell Phone Activities 2012, Pew Internet & American Life Project (Nov. 25, 2012).¹³ Syncing e-mail to a smartphone requires

¹⁰ http://www.cnet.com/8301-17918_1-10461614-85.html.

¹¹ <http://blog.nielsen.com/nielsenwire/?p=31688>.

¹² <http://www.apple.com/iphone/built-in-apps/>.

¹³

http://pewinternet.org/~media//Files/Reports/2012/PIP_CellActivities_11.25.pdf.

frequent connections even when the customer is not "using" the phone, and many services enable "push" e-mail to be delivered in "real time" to the device. See, e.g., Mail2Web, Mobile Email from mail2web.com Keeps You Connected (2012).¹⁴

In addition to smartphones, a range of other advanced devices can now access the Internet over cellular networks. Tablet computers such as the Apple iPad,¹⁵ the Amazon Kindle,¹⁶ and the Samsung Galaxy¹⁷ can all access data via cellular networks. Laptops can also access cellular networks via a wireless Internet card. See, e.g., AT&T, Wireless Internet Card Air Card (2012).¹⁸ As a result, users of these devices are also subject to the same location tracking technologies as cell phone users.

B. Current Technologies Can Precisely Locate a Device Using Network-based, Handset-based, or Third Party Methods

Current location tracking technology has evolved, in part, in response to federal communications regulations, which have

¹⁴ <http://mail2web.com/mobile-email/>.

¹⁵ See Apple, iPad with Wi-Fi + Cellular (2012), <http://www.apple.com/ipad/ultrafast-wireless/>.

¹⁶ See Kindle Fire HD 8.9: Faster Processor, Larger Screen, and 4G Coming Soon, CNET (Sept. 23, 2012), http://reviews.cnet.com/tablets/amazon-kindle-fire-hd/4505-3126_7-35438079.html.

¹⁷ See Samsung, Galaxy Tab 10.1 Feature, <http://www.samsung.com/global/microsite/galaxytab/10.1/feature.html> (last visited 12/18/12).

¹⁸

<https://www.wireless.att.com/businesscenter/solutions/wireless-laptop/modem-cards.jsp>.

sought to enable limited location tracking for use in emergencies, such as when a mobile user dials 911. As a result of these regulations, every cell phone service provider must be able to identify the location of a caller in an emergency for limited E-911¹⁹ purposes. See 47 C.F.R. § 20.18. But the use of this information is limited under the Federal Communications Act, which mandates that service providers protect consumer privacy by limiting disclosure of consumer proprietary network information ("CPNI"). See 47 U.S.C. § 222.²⁰ Service providers can satisfy this requirement by using either a network-based or handset-based method, so long as they meet the accuracy standards. See *id.* § 20.18(h). Law enforcement officers frequently demand access to the same accurate location data that service providers must be able to produce for E911 purposes. In addition, law enforcement officers can collect location data in real time using tracking devices and other third party records.

¹⁹ E-911 or "Enhanced 911" services facilitate emergency calls for wireless phones. See generally Fed. Commc'ns Comm'n, Enhanced 9-1-1 - Wireless Services <http://transition.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html> (last accessed Dec. 20, 2012).

²⁰ There are only three exceptions to the CPNI rule that allow disclosure of cell phone location information: (1) to an emergency 911 service, (2) to inform a legal guardian in an emergency, and (3) to assist in the delivery of emergency services. 47 U.S.C. § 222(d)(4).

1. Network-based Location Technologies

Network-based location tracking technologies rely on existing equipment to determine the location of a target device. See Ali H. Sayed, Alireza Tarighat & Nima Khajehnouri, Network-Based Wireless Location, IEEE Signal Processing Magazine 24, 26 (Jul. 2005).²¹ Cell phone networks consist of a series of antennas (or "cell sites"), which can be densely concentrated in urban areas with many users. See CTIA: The Wireless Association, Wireless in America: How Wireless Works (Jan. 2011).²² Mobile devices communicate with nearby cell sites during a process called "registration," which occurs automatically even when the device is idle. A Guide to the Wireless Engineering Body of Knowledge 77 (Andrzej Jajszczyk ed., 2nd ed. 2011).²³ During the registration process, mobile devices also communicate with nearby cell sites in order to identify the strongest signal. Michele Sequeira & Michael Westphal, Cell Phone Science: What Happens When You Call and Why 104 (2010). A similar process

²¹ Available at http://www.ee.ucla.edu/~tarighat/pdf/spm_05_location.pdf.

²² For definitions of relevant cell phone terminology, see CDMA Glossary, supra note 3.

²³ This registration occurs whenever a subscriber enters a new area, but periodic updates can also occur based on the service provider's configuration. See Küpper at 107. See also CDMA Glossary, supra note 3 (describing "Distance-Based Registration" as "[a]n autonomous registration method in which the mobile station registers whenever it enters a cell whose distance from the cell in which the mobile station last registered exceeds a given threshold.>").

occurs when a user moves from one cell to another while making a call. See Nishith D. Tripathi, Jeffrey H. Reed & Hugh F. VanLandingham, Handoff in Cellular Systems, IEEE Pers. Comm., Dec. 1998, at 26.²⁴ The service provider can also initiate the registration process. See CDMA Glossary, supra note 3 (describing "Non-Autonomous Registration" as "[a] registration method in which the base station initiates registration.").²⁵ Once registration occurs, the information is stored temporarily in service provider databases in order to route calls. Tripathi, supra, at 26. A log is also typically created every time a call is made or data downloaded. See Stephanie K. Pell & Christopher Soghoian, Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact, 26 Berkeley Tech. L.J. 117, 128 (2012) (these logs reveal "which particular cell site a phone was near at the time of the call.").

These cell site records are the most basic component of network-based location data. See Junhui Zhao & Xueue Zhang, Location-Based Services Handbook: Wireless Location Technology

²⁴ Available at <http://www.scss.tcd.ie/Hitesh.Tewari/papers/tripathi98.pdf>. See also note 23.

²⁵ This forced registration could have the same effect of locating a phone by calling it. This is typically referred to as "pinging." See, e.g., Susan Freiwald, Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact, 70 Md. L. Rev. 681, 704 (2011).

in Location-Based Services § 2.2.1 (Syed A. Ahson & Mohammad Ilyas eds., 2011).²⁶ The size of a “cell,” the area served by a cell site, can range from several miles to several meters. See Dimitris Mavrakis, Do We Really Need Femto Cells?, Vision Mobile (Dec. 1, 2007).²⁷ As a result, a cell site location record can reveal the location of a mobile device in a specific area (like a room in a house) or within a large area (like a neighborhood). The smaller the cell site, the more precise the cell site location data. In order to increase network capacity, as is necessary in dense urban areas, providers typically shrink the size of their cells. Id. In 2000, there were 97 million wireless subscriber connections and as of 2010 there were nearly 293 million. CTIA: The Wireless Ass'n, Wireless in America: Wireless Subscriber Statistics (May 2011). Over that same time period, the number of cell towers has increased from 95,733 to 251,618. Id. In response to increased network demand, small cells are becoming increasingly common. See Press Release, Small Cells Outnumber Traditional Mobile Base Stations, Small Cell Forum (Oct. 31, 2012).²⁸

²⁶ See also Küpper at 130 (referring to the process as “proximity sensing”). This is also referred to as the “Cell-Id” positioning method. Id. at 231.

²⁷ <http://www.visionmobile.com/blog/2007/12/do-we-really-need-femto-cells/>.

²⁸ <http://www.smallcellforum.org/newsstory-small-cells-outnumber-traditional-mobile-base-stations>.

Cell site data can also be collected for a specific cell site and time without an individual target. See, e.g., In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d), Nos. 12-670, 671, 672, 673, 674, 2012 WL 4717778 (S.D. Tex. Sept. 26, 2012) (rejecting a government request for bulk tower data). This information is referred to as a "tower dump." Id. at *1. Government investigators have argued that they should be allowed to collect such data and analyze it in order to locate possible targets present at a particular location and time (like a crime scene). Id. The problem, as one court noted, is that it requires collection of "data related to innocent people who are not the target of the criminal investigation." Id. at 4. At least one such application has been rejected because the Government had no protocol in place to handle this sensitive private data. See Id.

Network-based location information can also be collected using more advanced and precise methods. Service providers can identify the location of a wireless device by using triangulation (or "lateration") methods based on simultaneous signals from several base stations. See Ali H. Sayed, Network-Based Wireless Location at 26-29. See also Küpper at 131-136. Even more advanced methods consider the exact angle and time of arrival of each signal. See Küpper at 138-140, 144-148.²⁹ The

²⁹ One example of such a system is the U-TDoA system implemented by TruePosition and used by current mobile carriers. Michael S.

current advanced triangulation methods are capable of locating a mobile device within 50-120 meters, even in rural areas, and provide comparable accuracy to A-GPS in urban environments. See id. at 231 (table describing the accuracy of various cellular positioning methods).

2. Handset-based Location Technologies

The handset-based method involves locating a mobile device based on information provided by the device itself (such as GPS data). See Frank Van Diggelen, A-GPS: Assisted GPS, GNSS, and SBAS 292 (2009).³⁰ Most current phones contain GPS technology. See Berg Insight, GPS and Mobile Handsets 2 (March 2010). The Global Positioning System ("GPS") is a "constellation of orbiting satellites that provides navigation data to military and civilian users all over the world." U.S. Air Force, Global Positioning System Factsheet (Sept. 15, 2010).³¹ GPS receivers, like those in mobile devices, can use the satellite signals to calculate "extremely accurate, three-dimensional location information (latitude, longitude and altitude), velocity (speed and direction) and precise time." Id. However, buildings and other environmental factors in urban areas can reduce the

McAdoo, High-accuracy Location Technologies and How They Are Used in Mission-critical Solutions 2 (2009), available at <http://www.trueposition.com/white-papers/>.

³⁰ Handset-based location technology "requires the use of special location-determining hardware and/or software in a portable or mobile phone." Digglen at 292.

³¹ <http://www.af.mil/information/factsheets/factsheet.asp?id=119>.

accuracy of GPS location data. See Adam Gorski, Understanding GPS Performance in Urban Environments, AGI (Jan. 4, 2011).³²

Assisted GPS ("A-GPS") positioning now provides improved accuracy, lower power consumption, and reduced location acquisition time for compatible devices. Küpper at 225. The A-GPS process works by estimating a position using standard GPS triangulation, and then adjusting for corrections provided by a remote reference station connected to the network. Id. at 227. This allows for extremely accurate location information, to within 10 meters in outdoor rural areas. Id. at 231.

Mobile devices can also determine location based on surrounding Wi-Fi networks. See Axel Küpper, Location-Based Services: Fundamentals and Operation 234 (2005). There are several companies that maintain databases listing the approximate location of wireless networks. Pell & Soghoian, supra, at 131. These companies are known as "location aggregators." Ann Cavoukian & Kim Cameron, Wi-Fi Positioning Systems: Beware of Unintended Consequences 6 (June 2011).³³ See, e.g., Open WLAN Map.³⁴ Internet service providers, such as Google, also use Wi-Fi data to determine a user's location. See Google, Statement to Several National Data Protection Authorities (Apr.

³² <http://blogs.agi.com/agi/2011/01/04/understanding-gps-performance-in-urban-environments/>.

³³ Available at <http://www.ipc.on.ca/images/Resources/wi-fi.pdf>.

³⁴ <http://www.openwlanmap.org/?lang=en> (last visited Dec. 20, 2012).

27, 2010).³⁵ These Wi-Fi Positioning Systems cross reference the user's nearby Wi-Fi networks with the database in order to determine the user's approximate location. Id. See generally Cavoukian & Cameron, supra, at 6 (describing Wi-Fi Positioning methods). It is not clear whether service providers have access to Wi-Fi position data generated by mobile devices.

3. Third-Party Methods

In addition to the location tracking methods described above, which require law enforcement to collect data indirectly through the service provider, there are surveillance technologies that facilitate real-time tracking of a mobile signal directly.

One such tool is known as an "IMSI Catcher," "StingRay," or "Triggerfish," and is used to identify and measure the strength and location of a mobile signal. See Jennifer Valentino-Devries, Stingray Phone Tracker Fuels Constitutional Clash, Wall St. J., Sept. 22, 2011.³⁶ IMSI catchers mimic a wireless carrier's network tower and can send and receive all the same signals going to the cellular tower. See EPIC, EPIC v. FBI - Stingray /

³⁵ Available at http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/googleblogs/pdfs/google_submission_dpas_wifi_collection.pdf.

³⁶ <http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html>.

Cell Site Simulator (2012).³⁷ IMSI catchers can determine a specific cell phones location by measuring the signal strength of the cell phone from several locations and utilizing triangulation to pinpoint the cell phones location. *Id.* These tools can also be used to identify a device based on its location, rather than the opposite. See In re Application of the U.S. for an Order Authorizing the Use of a Pen Register and Trap and Trace Device, ___ F. Supp. 2d ___, 2012 WL 2120492 (S.D. Tex. 2012) ("by determining the identifying registration data at various locations in which the Subject's Telephone is reasonably believed to be operating, the telephone number corresponding to the Subject's Telephone can be identified."). At least one court has rejected an application to use such technology because the Government failed to address how they would deal with "information concerning seemingly innocent cell phone users," which would be recorded by the equipment. *Id.*

II. Reasonable Expectation of Privacy in Location of Modern Cell Phones Under Federal and State Constitutions

Cell phone users maintain constant contact with their cell phones throughout the day, and because the location of a user's cell phone inevitably reveals when a person is within protected spaces including their home. For this reason, all users have a reasonable expectation of privacy in their cell phone location

³⁷ <http://epic.org/foia/fbi/stingray/>.

under Federal and State constitutions. This analysis begins with the traditional Reasonable Expectation of Privacy test as applied by the United States Supreme Court. See Kyllo v. United States, 533 U.S. 27, 32-33 (2001).

A. Individuals Have a Reasonable Expectation of Privacy in the Location of Their Modern Cell Phones Under the Federal Constitution

The collection and use of location data implicates the Fourth Amendment as the data can expose personal information about location, movement, associations and activities in private spaces such as homes. Society recognizes that individuals have an objective expectation of privacy in this kind of information. A subscriber's reasonable expectation is not eliminated by their use of a cell phone, which is a basic component of modern life. The location data associated with a modern cell phone can be a valuable resource to investigators, but that does not diminish the important privacy interests of cell phone users. Law enforcement can obtain location information in one of two ways: (1) compelled disclosure from a service provider, and (2) direct interception and triangulation of the cell phone signal. Both of these methods implicate Fourth Amendment interests and can be distinguished from those in Smith v. Maryland, 442 U.S. 735 (1979), and United States v. Miller, 425 U.S. 435 (1976).

An individual's reasonable expectation of privacy in their location is grounded in a pair of United States Supreme Court cases, but has recently been revisited by the Court in United States v. Jones and by other federal and state courts. Congress has also affirmed the privacy of consumer location information. See, e.g., 47 U.S.C. § 222(f). The traditional analysis, based on 'enhanced physical surveillance' is currently adapting to accommodate advances in location tracking technology. The Court has recognized that "[w]hile it may be difficult to redefine the Katz test in some instances," it is nevertheless necessary to avoid permitting "police technology to erode the privacy guaranteed by the Fourth Amendment." Kyllo v. United States, 533 U.S. 27, 34 (2001).

The basic components of the reasonable expectation of privacy test, as described in Katz v. United States, 389 U.S. 347 (1967), are (1) the individual's subjective expectation of privacy and (2) society's willingness to recognize that expectation as reasonable. See Kyllo, 533 U.S. at 33. Traditional law enforcement location tracking methods rarely exceeded such expectations because they required physical surveillance. The Court held in a pair of 1980s cases that use of technology to enhance traditional physical surveillance did not violate the target's reasonable expectation of privacy so long as the target was in public view. See United States v.

Knotts, 460 U.S. 276 (1983) and Karo v. United States, 468 U.S. 705 (1984).

The Court's decision in Knotts was based primarily on the 'public' nature of the surveillance target's activities. As the Court described it, "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." Knotts, 460 U.S. at 281. In contrast, the Court recognized in Karo that because "residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by warrant," officers were not allowed to monitor when the "beeper was inside the house, a fact that could not have been visually verified." Karo, 468 U.S. at 715.

This "inside/outside" distinction outlined in Knotts and Karo controlled the installation and use of traditional "tracking devices" by law enforcement. See generally M. Wesley Clark, Cell Phones as Tracking Devices, 41 Val. U. L. Rev. 1413 (2007) (Senior DEA attorney outlining recent judicial treatment of tracking devices). However, that framework was altered by the Court's recent decision in United States v. Jones, 132 S. Ct. 945 (2012). Under the traditional approach, law enforcement "acts at its peril," Clark, supra, at 1465, whenever it uses an electronic tracking device, because it "may not monitor" such a device "in a private place without a warrant" under Karo. In re

Application of U.S. for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed], 402 F. Supp. 2d 597 (D. Md. 2005).³⁸

The Court in *Jones* changed the approach by holding that the installation and use of a GPS tracking device constituted a search under the Fourth Amendment. Jones, 132 S. Ct. at 949.

In addition to the primary holding in *Jones*, the concurring opinions of Justices Sotomayor and Alito provide a five-justice consensus for the conclusion that, at the very least, “longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring); id at 964 (Alito, J., concurring). See also Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 313 (2012). This view is supported by other recent federal and state opinions.³⁹ Thus the Court’s

³⁸ See, e.g., United States v. Williams, 650 F. Supp. 2d 633, 67-669 (W.D. Ky. 2009) (no search where GPS device was installed on exterior of vehicle and vehicle was tracked only on public roads, but outcome might have been “entirely different” if device had been installed or monitored while vehicle was located on private property).

³⁹ See State v. Zahn, 812 N.W.2d 490 (S.C. 2012); People v. Weaver, 12 N.Y.3d 433 (2009); State v. Jackson, 150 Wash.2d 251, 262 (2003); In re Application of U.S. for an Order Directing a Provider of Electronic Communications Service to Disclose Records to Government, 620 F.3d 304 (3d Cir. 2010); In re U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010); State v. Holden, 54 A.3d 1123 (Del. Super. Ct. 2010); Commonwealth v. Wyatt, 30 Mass.L.Rptr. 270 (Mass. Sup. Ct. 2012). As the New York Court of Appeals noted in *Weaver*:

opinions in Jones altered the Knotts - Karo framework in two important ways. First, investigators are no longer allowed to operate at their 'peril' by installing and monitoring tracking devices without prior Fourth Amendment justification.⁴⁰ Second, law enforcement can no longer justify warrantless location tracking solely on the basis of a target's movement on public thoroughfares.

Based on the Court's analysis in Jones and Karo, the statutory protections for electronic communications, and the capabilities of modern cell phones, this Court should recognize an individual's reasonable expectation of privacy in the location of their cell phone. As the Court's decision in Jones established, investigators cannot install or use tracking devices without satisfying Fourth Amendment requirements. Fourth Amendment standards are also applicable to the collection and use of cell phone location data as such data necessarily reveals

Disclosed in the data retrieved from the transmitting unit, nearly instantaneously with the press of a button on the highly portable receiving unit, will be trips the indisputably private nature of which it takes little imagination to conjure: trips 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.

Weaver, 12 N.Y.3d at 441-42.

⁴⁰ See Ariane de Vogue, Supreme Court Ruling Prompts FBI to Turn Off 3,000 Tracking Devices, Yahoo! News (Mar. 7, 2012), <http://news.yahoo.com/supreme-court-ruling-prompts-fbi-turn-off-3-154046722--abc-news.html>.

information about activities in private spaces. The results of the most recent Pew Internet survey highlight the extremely close attachment between most users and their cell phones. Of those surveyed, 44% sleep with their phones next to their bed to “make sure they didn’t miss any calls, text messages, or other updates” and 29% describe their phones as “something they can’t imagine living without.” Aaron Smith, The Best (and Worst) of Mobile Connectivity, Pew Internet & American Life Project (Nov. 30, 2012).⁴¹

Under Karo, location data that reveals information “about the interior of the premises” is private and protected by the Fourth Amendment. 468 U.S. at 715. Thus, any cell phone location information collected by law enforcement would likely implicate the user’s reasonable expectation of privacy. Congress implicitly recognized the private nature of such information when it passed the Communications Assistance for Law Enforcement Act (“CALEA”) in 1994, Pub. L. 103-414, 108 Stat. 4280, by making clear that “call-identifying information shall not include any information that may disclose the physical location of the subscriber” when acquired under the minimal pen register standard. 47 U.S.C. § 1002(a). It similarly recognized the privacy interests in location information when it excluded

⁴¹http://pewinternet.org/~media//Files/Reports/2012/PIP_Best_Worst_Mobile_113012.pdf.

information from a "tracking device" from its definition of "electronic communications" subject to mandatory disclosure by statute. See 18 U.S.C. § 2510(12)(D), § 3117.

Federal courts in the District of Columbia,⁴² Indiana,⁴³ Maryland,⁴⁴ New York,⁴⁵ Texas,⁴⁶ and Wisconsin⁴⁷ have ruled that service providers cannot be compelled to disclose real-time cell phone location data under the current pen register statute, 18

⁴² See In re The Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 132 (D.D.C. 2005).

⁴³ See In re U.S., Nos. 1:06-MC-6, 7, 2006 WL 1876847, at *1 (N.D. Ind. July 5, 2006).

⁴⁴ See In re Application, 439 F. Supp. 2d 456 (D. Md. 2006); In re U.S. for Orders Authorizing Installation and Use of Pen Registers, 416 F. Supp. 2d 390 (D. Md. 2006); In re Application of U.S. for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed], 402 F. Supp. 2d 597 (D. Md. 2005).

⁴⁵ See In re Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 384 F. Supp. 2d 562 (E.D.N.Y. 2005).

⁴⁶ See In re U.S., 441 F. Supp. 2d 816, 837 (S.D.N.Y. 2006) ("This statutory argument does not hinge upon the precision of the requested surveillance. If the dual theory were found to authorize the limited cell site data sought here, it must necessarily authorize far more detailed location information, such as triangulation and GPS data, which unquestionably implicate Fourth Amendment privacy rights."); In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) ("The government's hybrid theory, while undeniably creative, amounts to little more than a retrospective assemblage of disparate statutory parts to achieve a desired result.").

⁴⁷ See In re U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947 (E.D. Wisc. 2006).

U.S.C. § 3121 *et seq.*, even in connection with the mandatory disclosure provisions of ECPA, 18 U.S.C. § 2703(d).⁴⁸ The Court of Appeals for the Third Circuit has also ruled that a magistrate may require probable cause to order a provider to disclose historical location information under 18 U.S.C. § 2703(d). See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't, 620 F.3d 304, 320 (3d Cir. 2010). These statutory protections underscore society's overall desire to impose procedural safeguards on the disclosure of location information due to its private nature.

The fact that some subset of cell phone location records, such as those registering movement on public thoroughfares, might be considered unprotected under Knotts is insufficient to outweigh the overall privacy interest in cell phone location data. The Knotts framework is not workable in the cell phone context for several reasons. First, the location data is collected remotely and investigators have no way to know beforehand whether a target is on a public road or in a protected space. Second, the amount of location information generated by cell phones and modern tracking devices is

⁴⁸ The combination of the pen register and ECPA authorities to justify disclosure of cell phone location records is referred to as the "hybrid theory." See In re Application, 402 F. Supp. 2d at 600.

enormous, as the Supreme Court recognized in Jones. See 132 S. Ct. at 952 n.6 (“*Knotts* . . . reserved the question whether ‘different constitutional principles may be applicable’ to ‘dragnet-type law enforcement practices’ of the type that GPS tracking made possible here.”).

Studies of consumer behavior confirm that users have strong location privacy expectations, and are unwilling to share their personal location without prior consent. One study found that users wish to control access to their location information. See Janice Y. Tsai et al., Location-Sharing Technologies: Privacy Risks and Controls (2010).⁴⁹ Another study showed that users demand granular control over the location data that they share with third parties. See Michael Benisch et al., Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs, 15 *Personal & Ubiquitous Comp.* 679 (2011). When users find out about surreptitious monitoring of their location, they strongly object.⁵⁰

49

http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

⁵⁰ See, e.g., John R. Quain, Changes to OnStar’s Privacy Terms Rile Some Users, N.Y. Times Blog: Wheels (Sept. 22, 2011), <http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users>; Nick Bilton, Tracking File Found in iPhones, N.Y. Times, Apr. 20, 2011, available at <https://www.nytimes.com/2011/04/21/business/21data.html>.

B. An Individual's Reasonable Expectation of Privacy in the Location of Their Cell Phone Is Not Eliminated by the Third Party Doctrine Because Location Data Is Not Voluntarily Disclosed and It Is Protected Under the Communications Act

Having established that location data from modern cell phones contains private information, the remaining question is whether these records remain unprotected based on the third party doctrine, as outlined by the Supreme Court in Smith v. Maryland, 442 U.S. 735 (1979), and United States v. Miller, 425 U.S. 435 (1976). The third party doctrine is inapplicable to cell phone location records for the reasons outlined by the Court of Appeals for the Third Circuit in In re Application, 620 F.3d 304, 317. "A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." Id. "[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 user; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all." Id. at 317-[3]18.⁵¹

Congress has already recognized that consumers have a reasonable expectation of privacy in their cell phone location data. In the Wireless Communications and Public Safety Act of

⁵¹ See also United States v. Forest, 355 F.3d 942 (6th Cir. 2004), vacated and remanded on other grounds sub nom. Garner v. United States, 542 U.S. 1100 (2005).

1999, Pub. L. 106-81, 113 Stat. 1286 (1999), Congress amended the Communications Act and expressly protected wireless location information. Under the Act, a service provider cannot use or disclose "call location information concerning the user of a commercial mobile service" except with "express prior authorization of the customer" other than in accordance with the E-911 provisions. 47 U.S.C. § 222(f). The E-911 provisions make clear that location information is to be disclosed without prior authorization only in emergency circumstances. 47 U.S.C. § 222(d)(4).

C. Many State Supreme Courts Provide Privacy Protections at Least as Expansive as the Fourth Amendment, and New Jersey and Other States Explicitly Recognize Privacy Rights in Records Held by Third Parties

Most state constitutions contain protections for individual privacy that are at least as expansive as the Fourth Amendment. Stephen E. Henderson, Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search, 55 Cath. U. L. Rev. 373, 393 (2007). However, the privacy standards applicable under some state constitutions differ from Fourth Amendment standards in important ways relevant to an individual's reasonable expectation of privacy in cell phone location information.

Eleven states have rejected the third party doctrine in some form. Id. at 395.⁵² Other states have applied more stringent standards to the placement of location tracking devices even before Jones. See, e.g., Commonwealth v. Connolly, 454 Mass. 808 (2009); People v. Weaver, 12 N.Y.3d 433 (2009); People v. Oates, 698 P.2d 811, 816-818 (Colo. 1986). Some state courts have even gone so far as to recognize a reasonable expectation of privacy in cell phone location information explicitly. See, e.g., Commonwealth v. Wyatt, 30 Mass.L.Rptr 270 (Mass. Sup. Ct. 2012). Other courts disagree. See, e.g., People v. Hall, 86 A.D.3d 450 (N.Y. App. Div. 1st 2011). To the extent that other states recognize a constitutional privacy right at least as expansive as the Fourth Amendment, they should recognize that an individual has a reasonable expectation of privacy in the location of their cell phone under Jones and Karo as discussed in Part II.A. States that provide stronger protections for third party records, such as New Jersey, see State v. Hunt, 91 N.J. 338 (1982) (finding that phone toll billing records were

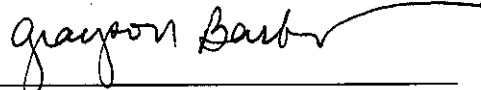
⁵² As Henderson describes, the states that "Reject the Federal Third-Party Doctrine" under his analysis are: California, Colorado, Florida, Hawaii, Idaho, Illinois, Montana, New Jersey, Pennsylvania, Utah, and Washington. Id. Specific case references can be found in Henderson's article on pages 396-399. Henderson also identified six states that "might reject" the third party doctrine: Alaska, Arkansas, Indiana, Massachusetts, Minnesota, New Hampshire, Oregon, South Dakota, Texas, and Vermont. Id. at 400-405.

protected), should be even more inclined to recognize the privacy of cell phone location records.

CONCLUSION

In light of this supplemental brief and the previous *amicus curiae* brief filed with this Court, EPIC urges this Court to find that an individual has a reasonable expectation of privacy in the location of their cell phone.

Dated: December 20, 2012



GRAYSON BARBER
Grayson Barber, LLC
68 Locust Lane
Princeton, NJ 08540
(609) 921-0391
*Counsel of Record for
Proposed Amicus Curiae
Electronic Privacy
Information Center*

MARC ROTENBERG
Electronic Privacy
Information Center
1718 Connecticut Ave NW
Suite 200
Washington, DC 20009
(202) 483-1140
*Appearing Pro Hac Vice
for Electronic Privacy
Information Center*