

COMMONWEALTH OF MASSACHUSETTS  
SUPREME JUDICIAL COURT

---

No. SJC-11482

---

COMMONWEALTH  
Plaintiff/Appellant

v.

SHABAZZ AUGUSTINE  
Defendant/Appellee



---

On Appeal from the Suffolk Superior Court

---

BRIEF OF ELECTRONIC FRONTIER FOUNDATION AS *AMICUS  
CURRIAE* IN SUPPORT OF DEFENDANT/APPELLEE

---

ELECTRONIC FRONTIER  
FOUNDATION

Hanni M. Fakhoury  
(CA# 252629)  
815 Eddy Street  
San Francisco, CA 94109  
Tel: (415) 436-9333  
Fax: (415) 436-9993  
hanni@eff.org

CYBERLAW CLINIC  
BERKMAN CENTER FOR  
INTERNET AND SOCIETY  
HARVARD LAW SCHOOL

Kit Walsh (BBO#673509)  
23 Everett Street, 2nd Floor  
Cambridge, MA 02138  
Tel: (617) 495-7547  
Fax: (617) 495-7641  
cwalsh@cyber.law.harvard.edu

**STATEMENT OF AMICUS CURIAE**

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), *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *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); *Commonwealth v. Rousseau*, 465 Mass. 372, 990 N.E.2d 543 (2013).

TABLE OF CONTENTS

INTRODUCTION ..... 1

ARGUMENT ..... 3

    I.    Historical Cell Site Information Reveals a  
          Detailed Map of a Person's Location Over  
          Time ..... 3

        A.    The Prevalence of Cell Phones Means The  
              Number of Cell Sites is Increasing .... 4

        B.    The Information Cell Site Data Can  
              Reveal Is Highly Sensitive ..... 10

    II.   Since People Have a Reasonable Expectation  
          of Privacy in their Location, the Fourth  
          Amendment and Article 14 Require Police  
          Obtain a Search Warrant to Acquire  
          Historical Cell Site Information ..... 14

        A.    The U.S. Supreme Court in *Jones* and  
              this Court in *Rousseau* Recognized an  
              Individual Has An Expectation of  
              Privacy In Their Location. .... 15

        B.    The Rationale in *Jones* and *Rousseau*  
              extends to the Commonwealth's  
              Acquisition and Use of Cell Site  
              Information ..... 21

    III.  A Warrant Requirement is the Proper Balance  
          Between Safeguarding Privacy and Permitting  
          Police Access to Cell Site Records ..... 23

CONCLUSION ..... 30

**TABLE OF AUTHORITIES**

**Federal Cases**

*Andresen v. Maryland*,  
427 U.S. 463 (1976) ..... 25

*Berger v. New York*,  
388 U.S. 41 (1967) ..... 25

*Brinegar v. United States*,  
338 U.S. 160 (1949) ..... 27

*Illinois v. Gates*,  
462 U.S. 213 (1983) ..... 27

*Illinois v. Lidster*,  
540 U.S. 419 (2004) ..... 29

*In re Appeal of Application for Search Warrant*,  
71 A.3d 1158 (Vt. 2012),  
cert. denied, 133 S. Ct. 2391 (2013) ..... 25

*In re Application for Pen Register & Trap/Trace  
Device with Cell Site Location Auth.*,  
396 F. Supp. 2d 747 (S.D. Tex. 2005) ..... 4, 5

*In the Matter of an Application of U.S. for an Order  
Authorizing the Release of Historical Cell-Site  
Info.*,  
809 F. Supp. 2d 113 (E.D.N.Y. 2011) ..... 1

*In the Matter of an Application of U.S. for an Order  
Authorizing Disclosure of Location Info. of a  
Specified Wireless Tel.*,  
849 F. Supp. 2d 526 (D. Md. 2011) ..... 1, 9, 13

*In the Matter of the 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) ..... 1, 23

*In re Application of U.S. for an Order for Prospective  
Cell Site Location Info. on a Certain Cellular  
Tel.*,  
460 F. Supp. 2d 448 (S.D.N.Y. 2006) ..... 13

<i>In re Application of U.S. for Historical Cell Site Data,</i>	
724 F.3d 600 (5th Cir. 2013) .....	1, 23
<i>Johnson v. United States,</i>	
333 U.S. 10 (1948) .....	27
<i>Katz v. United States,</i>	
389 U.S. 347 (1967) .....	3, 14, 18, 19
<i>Kyllo v. United States,</i>	
533 U.S. 27 (2001) .....	1, 3, 17
<i>Maryland v. Pringle,</i>	
540 U.S. 366 (2003) .....	27
<i>McDonald v. United States,</i>	
335 U.S. 451 (1948) .....	27
<i>Smith v. Maryland,</i>	
442 U.S. 735 (1979) .....	3
<i>United States v. Cuevas-Perez,</i>	
640 F.3d 272 (7th Cir. 2011) .....	28
<i>United States v. Garcia,</i>	
474 F.3d 994 (7th Cir. 2007) .....	3
<i>United States v. Jones,</i>	
132 S. Ct. 945 (2012) .....	<i>passim</i>
<i>United States v. Knotts,</i>	
460 U.S. 276 (1983) .....	15
<i>United States v. Lopez,</i>	
895 F. Supp. 2d 592 (D. Del. 2012) .....	19
<i>United States v. Maynard,</i>	
615 F.3d 544 (D.C. Cir. 2010) .....	2, 16, 17, 22
<i>United States v. Miller,</i>	
425 U.S. 435 (1976) .....	3
<i>United States v. Skinner,</i>	
690 F.3d 772 (6th Cir. 2012) .....	10, 11

*United States v. Warshak*,  
631 F.3d 266 (6th Cir. 2010) ..... 26

**State Cases**

*Commonwealth v. Blood*,  
400 Mass. 61, 507 N.E.2d 1029 (1987) ..... 14

*Commonwealth v. Connolly*,  
454 Mass. 808, 913 N.E.2d 356 (2009) ..... 19

*Commonwealth v. Donahue*,  
430 Mass. 710, 723 N.E.2d 25 (2000) ..... 24

*Commonwealth v. O'Day*,  
440 Mass. 296, 798 N.E.2d 275 (2003) ..... 24

*Commonwealth v. Ocasio*,  
434 Mass. 1, 746 N.E.2d 469 (2001) ..... 28

*Commonwealth v. Rousseau*,  
465 Mass. 372, 990 N.E.2d 543 (2013) .. 14, 19, 20,  
21

*Commonwealth v. Upton*,  
394 Mass. 363, 476 N.E.2d 548 (1985) ..... 14, 24

*In re Grand Jury Subpoena*,  
454 Mass. 685, 912 N.E.2d 970 (2009) ..... 14

*People v. Weaver*,  
12 N.Y.3d 433, 909 N.E.2d 1195 (2009) ..... 19

*State v. Campbell*,  
306 Or. 157, 759 P.2d 1040 (1988) ..... 19

*State v. Earls*,  
214 N.J. 564, 70 A.3d 630 (2013) ..... 11, 21, 22

*State v. Jackson*,  
150 Wash.2d 251, 76 P.3d 217 (2003) ..... 19

**Federal Statutes**

18 U.S.C. § 2703 .....passim

**State Statutes**

Mass. Gen. Laws Ann. ch. 276, § 3A .....25, 27

**U.S. Constitutional Provisions**

U.S. Const. amend. IV .....passim

**State Constitutional Provisions**

Massachusetts Declaration of Rights, Art. 14 ....passim

**Other Authorities**

Aaron Smith, *Smartphone Ownership – 2013 Update*, Pew Research Center,  
[http://pewinternet.org/~media/Files/Reports/2013/PIP\\_Smartphone\\_adoption\\_2013\\_PDF.pdf](http://pewinternet.org/~media/Files/Reports/2013/PIP_Smartphone_adoption_2013_PDF.pdf)..... 5

AT&T, *AT&T Advantages*,  
<http://www.att.com/shop/wireless.html#fbid=JqxsFviKiVc?tab2>.....9

CTIA - The Wireless Association, *Semi-Annual Wireless Industry Survey: Reported Wireless Data Traffic*,  
[http://files.ctia.org/pdf/CTIA\\_Survey\\_YE\\_2012\\_Graphics-FINAL.pdf](http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf)..... 6, 7

CTIA - The Wireless Association, *Wireless Quick Facts: Year-End Figures*,  
<http://www.ctia.org/advocacy/research/index.cfm/aid/10323>..... 5

General Data Resources, AntennaSearch.Com,  
<http://www.antennasearch.com/sitestart.asp?sourcepagename=reportviewer2&prevsessionidnum=214624746&prevordernum=1&previtemnum=1&sectionname=txreview&pagename=txreview&pagenum=1&cmdrequest=pagehandler>..... 8

Gyan Ranjan, et al., *Are Call Detail Records Biased for Sampling Human Mobility?*, 16 Mobile Computing & Comm. Rev., July 2012 .....6

Kim Zetter, *Anonymized Phone Location Data Not So Anonymous, Researchers Find*, *Wired*, March 27, 2013,  
[http://www.wired.com/threatlevel/2013/03/anonymou  
s-phone-location-data/](http://www.wired.com/threatlevel/2013/03/anonymou-s-phone-location-data/) ..... 12

Testimony of Matt Blaze, Associate Professor,  
University of Pennsylvania, *House Committee on  
the Judiciary Subcommittee on Crime, Terrorism,  
and Homeland Security Hearing on ECPA, Part 2:  
Geolocation Privacy and Surveillance*, April 25,  
2013. .... 4

Thomas A. O'Malley, *Using Historical Cell Site  
Analysis Evidence in Criminal Trials*, 59 *U.S.  
Attorneys' Bulletin.*, November 2011. .... 4

U.S. Attorney's Office, *Manhattan U.S. Attorney  
Announces Arrest of New York City Police Officer  
for Kidnapping Conspiracy and Illegally Accessing  
Federal Law Enforcement Database*, *F.B.I.*, October  
25, 2012  
[http://www.fbi.gov/newyork/press-  
releases/2012/manhattan-u.s.-attorney-announces-  
arrest-of-new-york-city-police-officer-for-  
kidnapping-conspiracy-and-illegally-accessing-  
federal-law-enforcement-database](http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-announces-arrest-of-new-york-city-police-officer-for-kidnapping-conspiracy-and-illegally-accessing-federal-law-enforcement-database)..... 10

Verizon Wireless, *Why Verizon?*, available at  
<http://www.verizonwireless.com/wcms/consumer/explore/why-verizon.html>..... 10

Yves-Alexandre de Montjoye, et al., *Unique in the  
Crowd: The privacy bounds of human mobility*,  
*Scientific Reports*, March 25, 2013  
[http://www.nature.com/srep/2013/130325/srep01376/  
full/srep01376.html](http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html) ..... 12



## INTRODUCTION

This Court has called upon *amicus curiae* to help it answer an important, disputed question that implicates the privacy of Massachusetts' citizens: "Whether there is a warrant requirement for cell phone records collected and held by the phone company, namely historical cell site location information, sought by police to establish a person's location at various times."<sup>1</sup>

The answer to this question requires this Court to confront the "power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). And little is more revealing than the pattern of a person's movements over time. As the D.C. Circuit recently said,

---

<sup>1</sup> Compare *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 559 (D. Md. 2011) (warrant required to obtain prospective GPS and cell site tracking data); *In the matter of an Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 119 (E.D.N.Y. 2011) (warrant required to obtain cell site tracking data) with *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 2013 WL 3914484, at \*12 (5th Cir. 2013) (warrant not required); *In the Matter of the 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, 319 (3d Cir. 2010) (warrant may be required by magistrate).

Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. 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).

Historical cell site information ("CSLI") is an increasingly popular law enforcement means of obtaining all of these details of a person's life. Its potential to intrude on a person's private life means this Court should answer its question with "yes": law enforcement must obtain a search warrant before obtaining historical CSLI from a cellular phone provider.

## ARGUMENT<sup>2</sup>

### **I. Historical Cell Site Information Reveals a Detailed Map of a Person's Location Over Time.**

As courts encounter evolving technologies, they must reject "mechanical interpretation[s] of the Fourth Amendment." *Kyllo*, 533 U.S. at 35-36. "The meaning of a Fourth Amendment search must change to keep pace with the march of science." *United States v. Garcia*, 474 F.3d 994, 997 (7th Cir. 2007) (citing *Katz v. United States*, 389 U.S. 347 (1967) and *Kyllo*, 533 U.S. at 34). Although the Commonwealth complains about the lower court's factual findings, there is no question that current cell phone technology is advancing to the point that historical cell site information can reveal an enormous amount of detail

---

<sup>2</sup> To be clear, in large part this case hinges on whether the so-called "third party doctrine" - the idea that an individual has no expectation of privacy in information they disclose to third parties - applies to historical cell site information. See *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *United States v. Miller*, 425 U.S. 435, 442-44 (1976). For the sake of not repeating what other *amici* will say on the issue, *amicus* notes that the lower court correctly ruled the "third party doctrine" does not apply since *Smith* and *Miller* contemplate far more limited and primitive records and a cell phone user does not "voluntarily" convey their detailed location information in a way that defeat a user's expectation of privacy in that information. See Augustine's Supplemental Record Appendix ("SRA") 272.

about a person's movements and locations. See Commonwealth's Opening Brief at 24.

A. The Prevalence of Cell Phones Means The Number of Cell Sites is Increasing.

A cell phone is a two-way radio that connects to a cellular network by sending radio signals to a nearby "cell site." See generally *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 750-52 (S.D. Tex. 2005).<sup>3</sup> A "cell site" consists of a cell phone tower, a radio transceiver and a base station controller. *In re Application for Pen Register*, 396 F. Supp. 2d at 750. The three directional antennas in a cell site divide the site into a number of "sectors" to handle communications to the cellular network.<sup>4</sup> When a cell phone is on, it "announces its presence to a cell tower via a radio signal." *In re Application for Pen*

---

<sup>3</sup> See also Testimony of Matt Blaze, Associate Professor, University of Pennsylvania, *House Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security Hearing on ECPA, Part 2: Geolocation Privacy and Surveillance*, April 25, 2013.

<sup>4</sup> Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials* 59 U.S. Attorneys' Bull. Nov. 2011, at 16, 19, available at [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usab5906.pdf](http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf).

*Register*, 396 F. Supp. 2d at 751. This process is known as "registration" or "identification." *Id.*

Cell phones are now ubiquitous in the United States. CTIA, the wireless cell phone trade association, reports that by December 2012, there were 326.4 million cell phones in the United States, meaning cell phones outnumber the population of the United States.<sup>5</sup> Earlier this year, the Pew Research Center reported that for the first time, a majority of American adults - 56% - owned Internet-enabled "smartphones" such as the Apple iPhone or Google's line of "Android" phones.<sup>6</sup> Smartphones are essentially miniature computers, allowing a user to check their email, access websites and even communicate with others over the phone's built in video camera.

Naturally, these Internet tasks have resulted in a significant increase in the amount of wireless data traffic being generated. CTIA reported the amount of

---

<sup>5</sup> CTIA - The Wireless Association, *Wireless Quick Facts: Year-End Figures*, available at <http://www.ctia.org/advocacy/research/index.cfm/aid/10323>.

<sup>6</sup> Aaron Smith, *Smartphone Ownership - 2013 Update*, p. 2, Pew Research Center, available at [http://pewinternet.org/~media//Files/Reports/2013/PIP\\_Smartphone\\_adoption\\_2013\\_PDF.pdf](http://pewinternet.org/~media//Files/Reports/2013/PIP_Smartphone_adoption_2013_PDF.pdf).

wireless data increased by 278% between 2010 and 2012.<sup>7</sup> The use of more data means there are more frequent connections to cell sites. This is particularly true with Internet enabled smartphones. In order to receive and download emails or perform other network functions, smartphone programs - known as applications or "apps" - remain running even when a user has the phone tucked away in their pocket or purse, and thus smartphones communicate with cell sites much more frequently than traditional cell phones.<sup>8</sup>

Most importantly for this Court, the growing demand for cell phones and especially smartphones has resulted in an explosion in the number of cell sites across the country. Nine months before the government

---

<sup>7</sup> CTIA - The Wireless Association, *Semi-Annual Wireless Industry Survey: Reported Wireless Data Traffic*, available at [http://files.ctia.org/pdf/CTIA\\_Survey\\_YE\\_2012\\_Graphics-FINAL.pdf](http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf).

<sup>8</sup> See Gyan Ranjan, *et al.*, *Are Call Detail Records Biased for Sampling Human Mobility?*, 16 *Mobile Computing & Comm. Rev.*, July 2012, at 3, 34 ("Unlike voice-calls and SMS activities, (user) data activities do not always require user initiation, nor user participation. For example, a plethora of applications running on 3G enabled cellular devices invoke themselves periodically or sporadically. These include push-mail notifications, periodic software updates and weather services, to name a few.") available at [http://www-users.cs.umn.edu/~granjan/Reports/MC2R\\_2012\\_CDR\\_Bias\\_Mobility.pdf](http://www-users.cs.umn.edu/~granjan/Reports/MC2R_2012_CDR_Bias_Mobility.pdf).

sought cell site information about Augustine's cell phone in September 2004, CTIA reported in December 2003 that there were approximately 162,986 cell sites in the United States. But by the end of 2012, there were 301,779 cell sites in the United States, an 85% increase in less than ten years.<sup>9</sup>

But in addition to faster connection speeds, this expansion in cell sites also means that a person's location can be pinpointed with greater precision. The precision of cell site data depends on the size of the sector. A sparsely populated rural area may only have one cell site servicing a wide geographical area. But a dense urban area would need many sectors and cell sites, each serving a smaller geographical area. The smaller the geographical area, the greater the ability to pinpoint a person's location accurately.

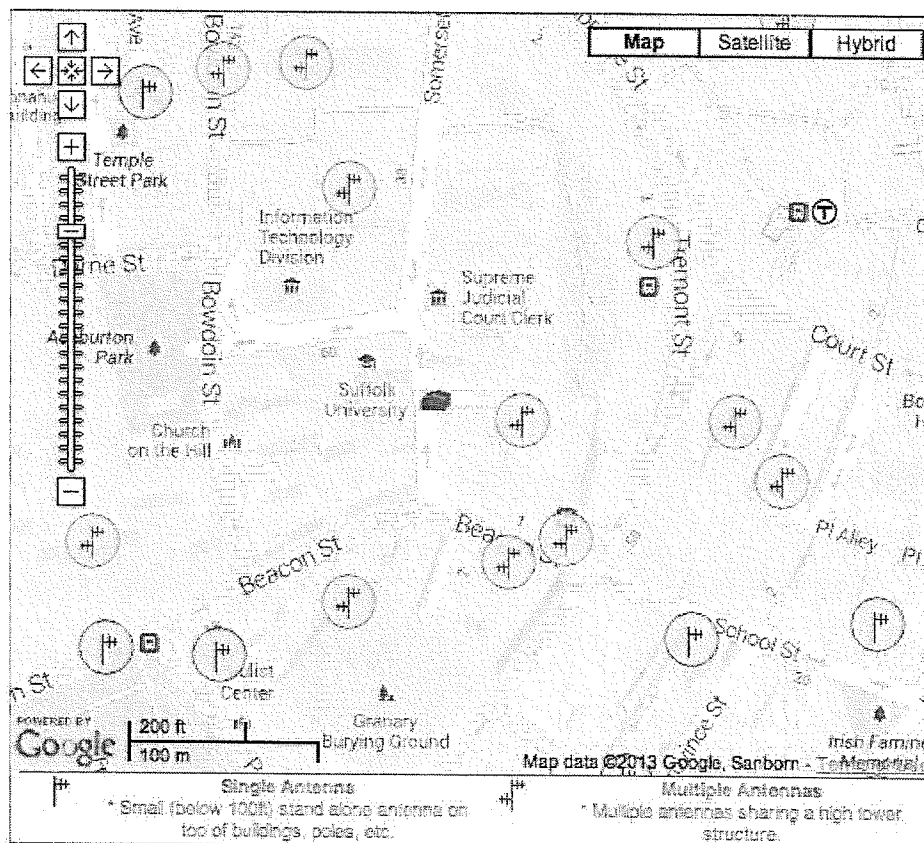
For example, a searchable database of publicly available cell tower and antenna information reveals there are approximately 907 antennas and 60 cell phone towers within a one mile radius of the John Adams

---

<sup>9</sup> CTIA - The Wireless Association, *Semi-Annual Wireless Industry Survey: Commercially-Operational Cell Sites in the U.S.*, available at [http://files.ctia.org/pdf/CTIA\\_Survey\\_YE\\_2012\\_Graphics-FINAL.pdf](http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf).

Courthouse at 1 Pemberton Square in Boston, Massachusetts.<sup>10</sup> In this dense urban area, knowing which tower or antenna a phone connected to would reveal on which side of Beacon Street a person was standing on when they made a call or received an email, or whether they were closer to Tremont or Somerset Street when they sent a text message.

Antenna Sites - (1 Pemberton Sq, Boston, MA 02108)



<sup>10</sup> General Data Resources, AntennaSearch.Com, Search conducted on September 20, 2013, available at <http://www.antennasearch.com/sitestart.asp?sourcepagename=reportviewer2&prevsessionidnum=214624746&prevorder num=1&previtemnum=1&sectionname=txreview&pagename=txreview&pagenum=1&cmdrequest=pagehandler>.



Despite the Commonwealth's complaints, there is no denying the lower court's fundamental premise: that location information derived from cell sites is already precise, and likely to become more so as demand for smartphones increases and technology improves. See also *In the Matter of an Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 534 (D. Md. 2011) ("Due to advances in technology and the proliferation of cellular infrastructure, cell-site location data can place a particular cellular telephone within a range approaching the accuracy of GPS.").<sup>11</sup>

---

<sup>11</sup> The Commonwealth's complaint about this premise ignores an obvious reason for this growth in cell sites and its corresponding precision. As more Americans use cell phones, particularly for data intensive activities like using the Internet, cell phone providers responded by expanding the amount of cell sites in order to handle the increased traffic. Investing in advanced technology to increase wireless speeds and improve service makes business sense, as the major cell phone providers use speed and coverage as a selling point to attract new customers and keep their existing customers happy. See, e.g., AT&T, *AT&T Advantages*, available at <http://www.att.com/shop/wireless.html#fbid=JqxsFviKiVc?tab2>. ("The nation's fastest and now most reliable 4G LTE network"); Verizon Wireless, *Why Verizon?*, available at <http://www.verizonwireless.com/wcms/consumer/explore/why-verizon.html> ("Verizon gives you the power to do it

B. The Information Cell Site Data Can Reveal Is Highly Sensitive.

While the Commonwealth complains about the lower court's belief as to the accuracy of cell site information, it ultimately wants warrantless access to this information specifically because of its precision. Cell site information aids law enforcement in pinpointing an individual near the scene of a crime. For example, in the high profile case of the "cannibal cop" Gilberto Valle, the FBI proudly and prominently announced that its agents used cell site information to place Valle within blocks of one of the alleged victim's home.<sup>12</sup>

Similarly, in *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), law enforcement was able to track a phone (and the person carrying it) almost 770 miles from Tucson, Arizona to Abilene, Texas over two days.

---

all, all on the largest high-speed wireless network in America.").

<sup>12</sup> U.S. Attorney's Office, *Manhattan U.S. Attorney Announces Arrest of New York City Police Officer for Kidnapping Conspiracy and Illegally Accessing Federal Law Enforcement Database*, F.B.I., October 25, 2012, available at <http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-announces-arrest-of-new-york-city-police-officer-for-kidnapping-conspiracy-and-illegally-accessing-federal-law-enforcement-database>.

See *Skinner*, 690 F.3d at 776.<sup>13</sup> Agents could see the suspect's travel point by point, and waited until he stopped at a rest stop before swooping in to arrest him. *Id.* Most critically, "[a]t no point did agents follow the vehicle or conduct any type of visual surveillance." *Id.* The cell phone did the surveillance for the agents in a safer and easier way. Agents would not need to follow the truck physically around the clock or run the risk that they would be discovered. Nor did they need to find a way to surreptitiously install a GPS device onto the truck to track its movements. Instead, as the New Jersey Supreme Court recently said, cell site information "is akin to using a tracking device and can function as a substitute for 24/7 surveillance without police having to confront the limits of their resources." *State v. Earls*, 214 N.J. 564, 586, 70 A.3d 630, 642 (2013).

---

<sup>13</sup> *Skinner* involved real time location tracking as opposed to historical location information. Both reveal an enormous amount of sensitive information about where a person goes and who they associated with. In fact, as the trial court correctly noted, historical location information arguably leads to an even more intrusive and novel government action: its ability to recreate a person's past movements. See SRA 274.

The monitoring that occurred here - at least 14 days worth of tracking Augustine's location - is far more invasive than the tracking in *Skinner*. Last year Supreme Court Justice Sotomayor cautioned that long-term location monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

This is not just a hypothetical concern. Earlier this year, a team including researchers from Harvard and MIT determined that it took just a minimal amount of location information gathered from anonymized cell phone location information to uniquely identify 95% of the users.<sup>14</sup> That is, armed with 15 months worth of anonymized mobile phone data of 1.5 million users, researchers could identify a specific individual with

---

<sup>14</sup> See Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The privacy bounds of human mobility*, Scientific Reports, March 25, 2013, available at <http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html>; see also Kim Zetter, *Anonymized Phone Location Data Not So Anonymous, Researchers Find*, Wired, March 27, 2013, available at <http://www.wired.com/threatlevel/2013/03/anonymous-phone-location-data/>.

merely four sets of hourly updates of which cell phone tower a person connected to. As the authors note, "the uniqueness of human mobility traces is high" and yet a cell phone makes this information easily accessible to the government.<sup>15</sup>

Cell phone tracking can even reveal information about a person in the most constitutionally protected space: a home. One federal magistrate judge has noted "pinging a particular cellular telephone will in many instances place the user within a home, or even a particular room of a home." *In the Matter of an Application of U.S. for an Order Authorizing Disclosure*, 849 F.Supp.2d at 540; see also *In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448, 462 (S.D.N.Y. 2006) (warning government's use of cell site data to "surveil a target in a private home that could not be observed from public spaces" could be unconstitutional).

Thus, given the sensitive details cell site information will typically reveal, it is clear that it must be safeguarded by requiring law enforcement

---

<sup>15</sup> Yves-Alexandre de Montjoye, *supra* note 14.

obtain a search warrant before accessing this information.

**II. Since People Have a Reasonable Expectation of Privacy in their Location, the Fourth Amendment and Article 14 Require Police Obtain a Search Warrant to Acquire Historical Cell Site Information.**

Both the Fourth Amendment to the United States Constitution and Article 14 of the Massachusetts Declaration of Rights prohibit "unreasonable" searches and seizures. A "search" occurs when the government either violates a "reasonable expectation of privacy" or trespasses onto private property for the purpose of obtaining information. *Jones*, 132 S. Ct. at 949-50. The "reasonable expectation of privacy" test is defined as an "actual (subjective) expectation of privacy" that "society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361 (Harlan, J., concurring); see also *In re Grand Jury Subpoena*, 454 Mass. 685, 688, 912 N.E.2d 970, 973 (2009) (*Katz* formulation of "reasonable expectation of privacy" applies to Article 14). This Court has made clear, however, that Article 14 "does, or may, afford more substantive protection to individuals than that which prevails" under the Fourth Amendment. *Commonwealth v. Blood*, 400 Mass. 61, 68 n.9, 507 N.E.2d 1029, 1033 n.9

(1987) (citing *Commonwealth v. Upton*, 394 Mass. 363, 371-73, 476 N.E.2d 548, 554-56 (1985)). Under both the Fourth Amendment and Article 14, individuals have an expectation of privacy in their location that mandates police obtain a search warrant before tracking a person's movements for an extended period of time.

A. The U.S. Supreme Court in *Jones* and this Court in *Rousseau* Recognized an Individual Has An Expectation of Privacy In Their Location.

The United States Supreme Court most recently addressed expectations of location privacy in *Jones*. Federal agents installed a GPS device without a search warrant underneath the car of a suspected drug dealer. *Jones*, 132 S. Ct. at 948. Agents tracked Jones' public movements for 28 days throughout the District of Columbia and Maryland. *Id.* Ultimately, Jones was arrested and convicted of conspiracy to distribute drugs, and sentenced to life in prison. *Id.* at 948-49. Defending the search on appeal before the D.C. Circuit, the government argued that *United States v. Knotts*, 460 U.S. 276 (1983) held that a person had no reasonable expectation of privacy in movements he exposed to the public while driving on public streets. *Maynard*, 615 F.3d at 556.

The D.C. Circuit rejected this argument, noting that *Knotts* did not contemplate the prolonged visual surveillance enabled by a GPS device. *Id.* *Knotts* was concerned with "movements during a discrete journey." *Id.* (citing *Knotts*, 460 U.S. at 283). Aggregating those movements, however, "reveals more - sometimes a great deal more - than does the sum of its parts," including "what a person does repeatedly, what he does not do, and what he does ensemble." *Maynard*, 615 F.3d at 558, 562. The key inquiry, then, was not whether another person can possibly discover the information, but whether a person *reasonably expects* that another person might actually discover the information. *Id.* at 559. While portions of a person's daily travels are often exposed to some people, pervasive and invasive surveillance has an entirely different character. The "whole of one's movements over the course of a month is not actually exposed to the public because the likelihood anyone will observe all those movements is effectively nil." *Id.* at 558. The result was thus an "unknown type of intrusion into an ordinarily and hitherto private enclave." *Id.* at 565.

The Supreme Court affirmed the D.C. Circuit on different grounds, finding the warrantless trespass



onto Jones' property for the purpose of obtaining information for a criminal investigation constituted a "search" under the Fourth Amendment. *Jones*, 132 S. Ct. at 954. Yet, all members of the Supreme Court noted the possibility that electronic monitoring of a person's location could violate a reasonable expectation of privacy. Justice Scalia's majority opinion stated "mere visual observation does not constitute a search," but cautioned it "may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy." *Id.* at 953-54. But the majority felt the facts of *Jones* did not require the Court to conclusively decide the issue. *Id.* at 954.

In concurring opinions by Justices Sotomayor and Alito, a majority of the Justices echoed the D.C. Circuit's concern with the capabilities of technology to cheaply and efficiently aggregate reams of data to create new and unknown intrusions into previously private places. See *Id.* at 956 (Sotomayor, J., concurring) and 963 (Alito, J., concurring in the judgment). To Justice Sotomayor, technology advances that make "available at a relatively low cost such a

substantial quantum of intimate information about any person" to the Government "may alter the relationship between citizen and government in a way that is inimical to democratic society." *Id.* at 956 (Sotomayor, J., concurring) (citations and quotations omitted). The fact that the government could obtain similar information through "lawful conventional surveillance techniques" rather than new technologies was not "dispositive" of the Fourth Amendment issue. *Id.*; see also *Kyllo*, 533 U.S. at 35, n.2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.")

With respect to location privacy specifically, the concurring opinions in *Jones* concluded that "longer term GPS monitoring . . . impinges on expectations of privacy." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring). Justice Sotomayor questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain . . . their political and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring). And Justice Alito

believed "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964 (Alito, J., concurring).

Both before and after *Jones*, other courts looking at GPS surveillance under the *Katz* expectation of privacy test have determined that GPS surveillance is a "search" under the Fourth Amendment. See *State v. Zahn*, 812 N.W.2d 490, 496 (S.D. 2012) (use of GPS to track a car for 26 days was a "search" under *Katz*); *United States v. Lopez*, 895 F. Supp. 2d 592, 602 (D. Del. 2012) (defendant had "reasonable expectation that the vehicles he was using would not be tracked by electronic surveillance" for 17 days). In addition, a number of state courts have found GPS surveillance to be a "search" under their state constitutions. See, e.g., *People v. Weaver*, 12 N.Y.3d 433, 909 N.E.2d 1195 (2009); *State v. Campbell*, 306 Or. 157, 759 P.2d 1040 (1988); *State v. Jackson*, 150 Wash.2d 251, 76 P.3d 217 (2003).

That includes this very Court. In *Commonwealth v. Rousseau*, 465 Mass. 372, 990 N.E.2d 543 (2013) this Court had to decide whether a passenger in a car had

standing to challenge the use of GPS surveillance installed in a car he did not own or possess. Ultimately, this Court had to rely on the *Katz* reasonable expectation of privacy test rather than the trespass rationale of *Jones* or this Court's earlier decision in *Commonwealth v. Connolly*, 454 Mass. 808, 913 N.E.2d 356 (2009), which ruled that "use and control" of defendant's car to track his location was a "search" under Article 14. See *Connolly*, 454 Mass. at 823, 913 N.E.2d at 370. Tellingly, in ruling the passenger did have standing, this Court in *Rousseau* expressly cited to Justice Sotomayor's concerns in her concurring opinion in *Jones* about how "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Rousseau*, 465 Mass. at 382, 990 N.E.2d at 553 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)). It concluded "that under art. 14, a person may reasonably expect not to be subjected to extended GPS electronic surveillance by the government, targeted at his movements, without judicial oversight and a showing of

probable cause." *Rousseau*, 465 Mass. at 382, 990 N.E.2d at 553.

B. The Rationale in *Jones* and *Rousseau* extends to the Commonwealth's Acquisition and Use of Cell Site Information.

While *Maynard*, *Jones*, and *Rousseau* all involve GPS surveillance, they are still applicable to the constitutionality of acquiring cell site location information. Ultimately, *Maynard*, the concurring opinions in *Jones*, and *Rousseau's* reliance on Justice Sotomayor's concurring opinion demonstrate that regardless of *how* electronic surveillance is conducted, people nonetheless maintain a reasonable expectation of privacy in their aggregated movements - even their public movements - since society would deem it unlikely that anything more than small, discrete movements would be observed at a time. That means individuals also have a reasonable expectation of privacy to be free from surveillance done through historical cell site records, thus triggering Article 14's requirement of a search warrant supported by probable cause and judicial oversight. See *Rousseau*, 465 Mass. at 382, 990 N.E.2d at 553.

The New Jersey Supreme Court recently applied such rulings about GPS surveillance to historical cell

site information in *State v. Earls*, 214 N.J. 564, 70 A.3d 630 (2013). There, police acquired cellphone tower data from T-Mobile without a search warrant. *Earls*, 214 N.J. at 570, 70 A.3d at 633-34. Looking at the issue under the New Jersey state constitution, the court found the warrantless acquisition unconstitutional. *Id.* at 570, 70 A.3d at 633. Critically, like the D.C. Circuit highlighted in *Maynard* and Justice Alito explained in his concurring opinion in *Jones*, the New Jersey high court believed cell site tracking involved "a degree of intrusion that a reasonable person would not anticipate." *Id.* at 586, 70 A.3d at 642 (citing *Jones*, 132 S. Ct. at 964 (Alito, J., concurring)). Ultimately, cell site data reveals a "broad range of personal ties with family, friends, political groups, health care providers, and others," details which "provide an intimate picture of one's daily life." *Earls*, 214 N.J. at 586, 70 A.3d at 642 (citing *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring)).

This Court should reach the same conclusion as *Earls*. Whether done through GPS or cell sites, continuously tracking a person's movement triggers an expectation of privacy that requires a search warrant.

**III. A Warrant Requirement is the Proper Balance Between Safeguarding Privacy and Permitting Police Access to Cell Site Records.**

Finally, this Court should not fear that imposing a search warrant requirement would result in an unnecessary burden on law enforcement's ability to use historical cell site information to solve crimes.

To get Augustine's cell site records, the government went to a magistrate and applied for an order under the Stored Communications Act ("SCA"), specifically 18 U.S.C. § 2703(d). See SRA 15-16, 151-152. But that section specifically states, "[i]n the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State." 18 U.S.C. § 2703(d). In other words, federal law expressly permits states to impose more stringent access requirements to state law enforcement officials.<sup>16</sup>

---

<sup>16</sup> Even when it comes to federal law enforcement officers, the Third Circuit has ruled that 18 U.S.C. § 2703(d) gives magistrates discretion to require a search warrant in some instances before authorizing access to historical cell site location information. *In re Application of U.S. for an Order*, 620 F.3d at 319 (§ 2703 gives magistrate "the option to require a warrant showing probable cause."); *but see In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 2013 WL 3914484, at \*5-6 (disagreeing with Third Circuit).

Even getting an order under 18 U.S.C. § 2703(d) requires law enforcement to get approval from a judge. Under § 2703(d), the government must demonstrate to the court "specific and articulable facts showing that there are reasonable grounds to believe . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Functionally, obtaining a § 2703(d) order is no different than getting a search warrant. Both involve *ex parte* proceedings before a magistrate, who hears the facts known to law enforcement by way of affidavit and affirmation to determine whether the appropriate legal standard has been met.

A search warrant requirement would only make two changes to the procedure contemplated under § 2703(d). First, it would change the legal standard that must be met before the government can get access to these records. Instead of demonstrating the records are "relevant and material," the government would have to convince the magistrate there was "probable cause," or a "substantial basis to conclude that a crime had been committed" and "that the items described in the warrant were related to the criminal activity and probably in the place to be searched." *Commonwealth v.*



*O'Day*, 440 Mass. 296, 298, 798 N.E.2d 275, 278 (2003) (citing *Commonwealth v. Donahue*, 430 Mass. 710, 715, 723 N.E.2d 25, 30 (2000) and *Commonwealth v. Upton*, 394 Mass. 363, 370, 476 N.E.2d 548, 554 (1985)).

Second, the magistrate would have greater authority to supervise the execution of a search warrant. The Supreme Court has explained that when it comes to searches, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). When it comes to electronic surveillance in particular, warrants typically have "minimization" requirements that limit electronic surveillance to ensure "similar protections to those that are present in the use of conventional warrants authorizing the seizure of tangible evidence." *Berger v. New York*, 388 U.S. 41, 57 (1967); see also *In re Appeal of Application for Search Warrant*, 71 A.3d 1158, 1170 (Vt. 2012), cert. denied, 133 S. Ct. 2391 (2013). And with search warrants, officers are required to return to the magistrate within seven days of execution with a return of what evidence they obtained. See, e.g., Mass. Gen. Laws Ann. ch. 276,

§ 3A ("Every officer to whom a warrant to search is issued shall return the same to the court by which it was issued . . . with a return of his doings thereon").

Yet these minor differences between an order issued under § 2703(d) and a search warrant are constitutionally significant. The Commonwealth argues that the fact it went to a court to obtain an order under § 2703(d) means this Court is not "presented [with] the typical 'warrantless' search." Commonwealth's Opening Brief at 48. But while it is true officers did get a judicial order, they did not get a search warrant supported by probable cause to access the cell site records. A search subject to a judicial order unsupported by probable cause is nonetheless a "warrantless" search for purposes of the Fourth Amendment and Article 14. In *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) the Sixth Circuit ruled that the government's use of a subpoena and § 2703(d) order to access emails violated the Fourth Amendment notwithstanding the fact the text of the Stored Communications Act authorized warrantless access. 631 F.3d at 283, 288. It simply found that "to the extent that the SCA purports to permit the

government to obtain such emails warrantlessly, the SCA is unconstitutional." *Id.* at 288. The same situation is true here: all that matters for purposes of the constitutional question before this Court is whether officers obtained a search warrant supported by probable cause. The absence of a warrant makes the seizure and subsequent search of Augustine's location information unconstitutional.

Ultimately, while these differences impose a minimal additional burden upon law enforcement, they play an important role in limiting police searches and safeguarding privacy. The probable cause standard "protects 'citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime.'" *Maryland v. Pringle*, 540 U.S. 366, 370 (2003) (quoting *Brinegar v. United States*, 338 U.S. 160, 176 (1949)). Judicial supervision over the warrant process is important too, as the "the Fourth Amendment has interposed a magistrate between the citizen and the police . . . so that an objective mind might weigh the need to invade that privacy in order to enforce the law." *McDonald v. United States*, 335 U.S. 451, 455 (1948); see also *Illinois v. Gates*, 462 U.S. 213, 240 (1983) (the "essential protection" of

the Fourth Amendment warrant requirement is for evidentiary inferences to "be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.'" (citing *Johnson v. United States*, 333 U.S. 10, 13-14 (1948)). Even the return requirements in Mass. Gen. Laws Ann. ch. 276, § 3A serve the important goal of providing "defense counsel with access to the warrant and all corresponding documents supporting the issuance of the warrant" so that the defendant can adequately prepare a defense and raise potential challenges to state's collection of evidence. *Commonwealth v. Ocasio*, 434 Mass. 1, 5, 746 N.E.2d 469, 473 (2001).

When it comes to new surveillance technology, judicial oversight is especially important to ensure the invasive capabilities of new technologies do not "alter the relationship between citizen and government in a way that is inimical to democratic society." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)). Long term electronic surveillance poses the serious risk of upsetting the traditional relationship between citizen

and state by avoiding what has long been the "greatest protection[] of privacy": "practical" restraints such as the cost and difficulty of maintaining long-term, covert surveillance. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring). Since cell site surveillance, like GPS monitoring, "is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" *Id.* at 956 (Sotomayor, J., concurring) (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004)). Judicial oversight must provide this crucial check on law enforcement as technology eradicates the more traditional restrictions on police power.

Finally, the fact the Commonwealth has claimed that the affidavit submitted in support of the request for a § 2703(d) order established probable cause shows why a search warrant requirement is not an additional burden. Commonwealth's Opening Brief at 56. Assuming the state is correct that the facts presented rise to the level of probable cause, all officers in the state could do exactly what the officers did here in order to get evidence and make an arrest. Imposing a

probable cause standard would still permit police officers to do their jobs while ensuring privacy interests in a person's location are not easily trampled upon.

### CONCLUSION

Historical cell site information is a valuable crime-fighting tool because of its power to intrude on a traditionally private sphere to obtain an enormous amount of sensitive information about where a person has been, their patterns of movements and their associations and affiliations. Law enforcement should be permitted to use this information to keep people safe, provided they adhere to strict safeguards designed to protect privacy.

The proper way to safeguard privacy while maintaining law enforcement access to this evidence is to require a search warrant supported by probable cause before authorizing disclosure of cell site location information. This strikes the right balance between privacy and security by ensuring a magistrate is satisfied there is a substantial basis to believe a crime has been committed and cell site information would probably lead to evidence related to the criminal activity.

Because the lower court correctly balanced these interests, its decision should be affirmed.

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION

BY ITS COUNSEL<sup>17</sup>



---

Kit Walsh (BBO#673509)  
Clinical Instructional Fellow, Cyberlaw Clinic  
Berkman Center for Internet and Society  
Harvard Law School  
23 Everett Street, 2nd Floor  
Cambridge, MA 02138  
Tel: (617) 495-7547 / Fax: (617) 495-7641  
Email: cwalsh@cyber.law.harvard.edu

ON THE BRIEF:

Hanni M. Fakhoury (CA# 252629)  
Electronic Frontier Foundation  
815 Eddy Street  
San Francisco, CA 94109  
Tel: (415) 436-9333  
Fax: (415) 436-9993  
Email: hanni@eff.org

DATED: September 23, 2013

---

<sup>17</sup> Amicus thanks Harvard Law School Cyberlaw Clinic student Margaret Lenahan for her valuable contributions to this brief.

CERTIFICATE OF COMPLIANCE

I, Kit Walsh, hereby certify pursuant to Mass. R. App. P. 16(k) that the instant brief complies with the rules of court pertaining to the filing of briefs, including, but not limited to, Mass. R. App. P. 16(a)(6), (b), (e), (f), and (h), 18, and 20.

Dated: September 23, 2013

Kit Walsh



## ADDENDUM

### **Constitution of the United States Amendment IV**

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

### **Constitution of the Commonwealth of Massachusetts Article XIV**

Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.

### **Mass. Gen. Laws Ann. ch. 276, § 3A**

#### § 3A. Time for return of warrant

Every officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event not later than seven days from the date of issuance thereof, with a return of his doings thereon; provided, however, that a justice of the superior court may at any time receive complaints and issue search warrants returnable in seven days before a district court named in such warrant and in that event the officer shall make his return to such district court as directed.

**18 U.S.C. § 2703**

§ 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.--

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a

wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

CERTIFICATE OF SERVICE

I, Kit Walsh, hereby certify that on September 23, 2013, I caused two true and correct copies of the above document to be served on counsel of record for each other party by mailing the document by first-class mail, postage pre-paid, to the following:

Cailin M. Campbell  
Office of the District Attorney/Suffolk  
One Bulfinch Place  
Third Floor  
Boston, MA 02114  
617-619-4082

Matthew R. Segal  
Jessie J. Rossman  
American Civil Liberties Union Foundation of  
Massachusetts  
211 Congress Street  
Boston, MA 02110  
617-482-3170

Nathan F. Wessler  
American Civil Liberties Union Foundation  
125 Broad Street, 18th Floor  
New York, NY 1004  
212-549-2500

Dated: September 23, 2013

Kit Walsh

