COMMONWEALTH OF MASSACHUSETTS

SUPREME JUDICIAL COURT

No. SJC-12499

COMMONWEALTH OF MASSACHUSETTS,

Appellant,

v.

JEROME ALMONOR,

Appellee.

ON APPEAL FROM BROCKTON SUPERIOR COURT

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS, INC. and MASSACHUSETTS ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

Christopher T. Holding
(BBO# 600627)
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, MA 02210
Tel.: 617.570.1000
Fax.: 617.523.1231
CHolding@goodwinlaw.com

Matthew R. Segal
(BBO# 654489)
Jessie J. Rossman
(BBO# 670685)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS, INC.
211 Congress Street
Boston, MA 02110
Tel: 617-482-3170
msegal@aclum.org

Counsel for Amici Curiae
(Additional counsel listed on inside cover)

Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: 415-436-9333
jlynch@eff.org

Chauncey B. Wood
(BBO# 600354)
WOOD & NATHANSON, LLP
50 Congress Street, Ste. 600
Boston, MA 02109
Tel.: 617.776.1851
cwoodesq@gmail.com

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutions and Statutes

Other Authorities

INTRODUCTION

This case arises from the Commonwealth's warrantless acquisition of precise real-time location information from a cell phone. That acquisition violated article 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the United States Constitution.

Cell phones generate location data automatically, because that data is a byproduct of turning on or using a phone, and inevitably, because phones are essential parts of modern life. But phones can also be *forced* to generate precise location data on demand, at the direction of law enforcement. And that is what happened here. Without securing a warrant, a police officer directed Jerome Almonor's cell phone carrier to deliver "Precision Location" data for his phone. RA 68. The carrier appears to have then "pinged" the phone, causing it to generate information that revealed its location, and thus Mr. Almonor's location. And that location, according to coordinates the carrier reported to the officer, was in a private home. RA 64-65, 68, 72-73; *see also* Almonor Br. 12.

For two reasons, this acquisition of precise real-time phone location information violated article 14 and the Fourth Amendment. First, by warrantlessly ascertaining Mr. Almonor's location in a private home, the Commonwealth intruded on his constitutionally-

protected *privacy interests*. *See Commonwealth v. Augustine*, 467 Mass. 230 (2014); *Commonwealth v. Estabrook*, 472 Mass. 852 (2015); *Carpenter v. United States*, 138 S. Ct. 2206 (2018). Second, by warrantlessly operating Mr. Almonor's phone in order to track his location, the Commonwealth interfered with the security of his person, papers, effects, or possessions under art. 14 and the Fourth Amendment, and thus intruded on his constitutionally-protected *property interests*. *See Commonwealth v. Connolly*, 454 Mass. 808 (2009); *United States v. Jones*, 565 U.S. 400 (2012); *see also Carpenter*, 138 S. Ct. at 2268-72 (Gorsuch, J., dissenting).

The Commonwealth argues otherwise. It contends that it can warrantlessly leverage cell phones to pinpoint the location of any person, at any time, at any place, for up to six hours. *See* Comm. Br. 13-21. As shown below, the magnitude of this intrusion cannot be overstated. But it can, and should, be rejected.

STATEMENT OF THE ISSUES

1. As the lower court held, did the Commonwealth's acquisition of Mr. Almonor's precise real-time location information from his cell phone, created at the direction of the government, violate privacy interests protected by art. 14 and the Fourth Amendment?

2. By warrantlessly directing Mr. Almonor's phone to reveal its location, and thus his location, did the Commonwealth unreasonably interfere with his constitutionally-protected property interests, in violation of art. 14 and the Fourth Amendment?

STATEMENT OF INTEREST OF AMICI

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for nearly 30 years. With more than 40,000 active donors, including donors in Massachusetts, EFF represents technology users' interests in court cases and broader policy debates. EFF has served as amicus in numerous cases addressing Fourth Amendment protections for cell phone location information, including *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018)(amicus brief cited in opinion); *Commonwealth v. Augustine*, 467 Mass. 230 (2014); *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); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015); *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015); *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016); and *State v. Andrews*, 134 A.3d 324, 349 (Md. Ct. Spec. App. 2016).

The American Civil Liberties Union of Massachusetts, Inc. (ACLUM), an affiliate of the national ACLU, is a statewide membership organization dedicated to the principles of liberty and equality embodied in the constitutions and laws of the Commonwealth and the United States. The rights that ACLUM defends through direct representation and amicus briefs include the right to be free from unreasonable searches and seizures. *See, e.g.*, *Augustine*, 467 Mass. 230; *Commonwealth v. Johnson*, SJC-12483 (Mass. amicus brief filed Aug. 13, 2018).

The Massachusetts Association of Criminal Defense Lawyers (MACDL) is the Massachusetts affiliate of the National Association of Criminal Defense Lawyers and an incorporated association representing more than 1,000 experienced trial and appellate lawyers who are members of the Massachusetts Bar and who devote a substantial part of their practices to criminal

defense. MACDL devotes much of its energy to identifying, and attempting to avoid or correct, problems in the Commonwealth's criminal justice system, including by filing amicus curiae briefs in cases raising questions of importance to the administration of justice.

STATEMENT OF THE CASE

Amici adopt appellee's statement of the facts and provide the following information concerning the relevant technologies.

I. Cell Phones

Owning a cell phone is not a luxury. Ninety-five percent of Americans have one, and most carry their phone with them everywhere they go.[1] The first commercial cell phone service in the U.S. was offered in 1983.[2] Now, according to a recent estimate, "[t]here are 396 million cell phone service accounts in the United States — for a Nation of 326 million people." *Carpenter*, 138 S. Ct. at 2211.

More than 77 percent of Americans now own smartphones; these phones can send email and take

---

[1] *See Mobile Fact Sheet*, Pew Research Center (January 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.

[2] Marguerite Reardon, *Cell Phone Industry Celebrates Its 25th Birthday*, CNET (Oct. 13, 2008), https://www.cnet.com/news/cell-phone-industry-celebrates-its-25th-birthday.

pictures, and include additional software like internet browsers, mapping applications, news services, social media tools, and games.[3] Because smartphones can send and receive much more data than older phones, the amount of data transferred over wireless networks via cell towers (also known as "cell sites") has increased significantly — more than 3,500 percent between 2010 and 2016 alone[4] — and service providers have installed more towers to handle that increase.[5]

II. Location Tracking

Increased cell phone use creates increasingly granular and detailed data about the location and movements of the people who use them. The data is not only a byproduct of owning and carrying a phone — collected by and stored with third-party service providers — but it may also be generated at law enforcement request by those same service providers, without the user's knowledge or permission.

---

[3] *Mobile Fact Sheet*, Pew Research Center; CTIA 2016 Survey, at 2.

[4] CTIA 2016 Survey at 8 (388 billion megabytes in 2010, 13,719 billion megabytes in 2016).

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

Cellular service providers can precisely locate cell phones upon law enforcement request. This capability stems from rules adopted in 1996 and implemented by 2001, under which the FCC required these providers to have "the capability to identify the latitude and longitude of a mobile unit making a 911 call."[6] This mandated location-tracking capability is increasingly precise. In January 2015, the FCC adopted new rules to increase law enforcement's ability to locate callers when they are indoors,[7] and to require service providers to develop techniques to determine a phone's altitude, and thus on which floor of a building it is located.[8]

Although this capability was developed initially to assist law enforcement in responding to 911 calls, service providers now provide the same location information in response to investigative requests. Law enforcement can ask a provider to generate new,

---

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

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

[8] Wireless E911 Order at 3-4.

precise, prospective location data by acquiring information from the target's phone, either "on demand or at periodic intervals."[9] Some providers send periodic location updates via email, while others allow law enforcement "direct access to users' location data" by logging into an "automated . . . web interface." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of r'hrg); *see also Maryland Real-Time Order,* 849 F. Supp. 2d 526, 531 (D. Md. 2011) (detailing Sprint's "Precision Locate Service").[10]

A phone can be located and tracked in real time regardless of whether it is in use. As long as the phone is on, law enforcement can request that the provider engage location-tracking capabilities; a user cannot disable this functionality.[11] Even modifying a phone's location-privacy settings does not disable the carrier's ability to determine the phone's precise location in real time. While these settings prevent

---

[9] Matt Blaze, *How Law Enforcement Tracks Cellular Phones*, Exhaustive Search (Dec. 13, 2013), http://www.mattblaze.org/blog/celltapping/.

[10] *See also* Sprint, *Legal Compliance Guidebook* 7 (2008), *at* https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_concordpd_concordnc.pdf at 568 (guide to requesting precision location from Sprint).

[11] *See, e.g. E911 Compliance FAQs*, Verizon Wireless, http://www.verizonwireless.com/support/e911-compliance-faqs/.

third-party applications ("apps," like Google Maps) from accessing the phone's location information, they do not prevent the carrier from locating the device.

Providers can obtain the location of a cell phone upon law enforcement request (1) by using hardware built into the phone ("handset-based" technology), or (2) by analyzing the phone's interactions with cell sites ("network-based" technology).[12] In this case, the Commonwealth directed Sprint to provide "Precision Location of mobile device (GPS Location)." RA 68. Therefore, the relevant technologies involve handset-based GPS pre-installed on Mr. Almonor's phone. This provided the Commonwealth with the precise GPS coordinates of Mr. Almonor's phone in real time and revealed his location inside a private home. RA 64-65.

Handset-based technology uses a mobile device's "special hardware that receives signals from a constellation of" GPS satellites.[13] This technology calculates the longitude and latitude of the phone in real time based on the timing of radio signals from satellites orbiting the earth.[14] The GPS chip installed

---

[12] 2013 Blaze Statement, *supra* n.5.

[13] *Id.* at 7; Wireless E911 Order at 5 n.11.

[14] ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 20-21 (2010) (statement of Matt Blaze, Associate

in the phone calculates its own location to within 10 meters, or approximately 33 feet.[15] Newer receivers, with enhanced communication-to-ground-based technologies that correct signal errors, can identify location within three meters or better and have a vertical accuracy of 5 meters or better 95 percent of the time.[16] GPS accuracy can be enhanced with "dual-frequency receivers" or augmentation systems, which allow for real-time positioning within a few centimeters.[17]

Service providers do not typically maintain GPS coordinate records for phones using their networks,

---

Professor, University of Pennsylvania) ("2010 Blaze Statement").

[15] 2013 Blaze Statement, *supra* n.5, at 7; Schneider, *supra* n.3; *see also Maryland Real-Time Order*, 849 F. Supp. 2d at 540-41 ("GPS location data . . . would likely place a cellular telephone inside a residence, at least where law enforcement have information regarding the coordinates of the home.") (citing U.S. Census Bureau, Median and Average Square Feet of Floor Area in New Single-Family Houses Compared by Location, *available at* http://www.census.gov/const/C25Ann/sftotalmedavgsqft.pdf)

[16] This is sometimes referred to as Assisted GNSS or A-GNSS. Jari Syrjärinne & Lauri Wirola, *Quantifying the Performance of Navigation Systems and Standards for Assisted-GNSS*, InsideGNSS, Sept./Oct. 2008, *available at* http://www.insidegnss.com/node/769; *What is GPS?*, Garmin, http://www8.garmin.com/aboutGPS/; *see also* U.S. Dept. of Defense, *Global Positioning System Standard Positioning Service Performance Standard* v (4th ed. Sept. 2008).

[17] GPS Accuracy, "How Accurate is GPS?" GPS.gov, http://www.gps.gov/systems/gps/performance/accuracy/.

but, upon law enforcement request, they can remotely activate a phone's GPS functionality and then cause the phone to transmit its coordinates back to the provider. *Maryland Real-Time Order,* 849 F. Supp. 2d at 534. This is sometimes called "pinging," and it can be done "unobtrusively, i.e., without disclosing to a telephone user the existence either of the Carrier's signal requesting the telephone to send a current GPS reading or that telephone's response." *Id.* at 535.[18]

If a phone cannot calculate its GPS coordinates, the service provider will "fall back" to a network-based location calculation.[19] Network-based technologies use existing cell site infrastructure, including cell towers, to identify and track location by silently "pinging" the phone and then triangulating its precise location based on which cell sites receive the reply transmissions.[20] Service providers can obtain this cell site location information even when no call is in process. *Maryland Real-Time Order,* 849

---

[18] This information can be generated upon government request at regular intervals or in near-real time. *See supra* n.9.

[19] Third Notice at 2429 n.306.

[20] 2013 Blaze Statement at 12; Stephanie Pell & Chris Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 Berkeley Tech. L. J. 117, 128 (2012).

F. Supp. 2d at 534.[21] Law enforcement officers can then locate someone in real time while they sit at a computer, and, though this did not happen in this case, even "follow" the suspect's movements over time.

III. The rise of real-time tracking

Real-time cell phone location information permits law enforcement to track people in ways that were previously impossible. For example, officers can now undertake tracking when they do not know who they are looking for. Authorities have found a suspect using electronic tracking when they "did not know the identity of their suspect, the specific make and model of the vehicle he would be driving, or the particular route by which he would be traveling." *United States v. Skinner*, 690 F.3d 772, 786 (6th Cir. 2012) (Donald, J., concurring in part).

Law enforcement agencies routinely demand real-time location information, and the number of these demands is staggering. Sprint implemented 59,762 demands for real-time location data in 2017, and

[21] Citing *The Collection and Use of Location Information for Commercial Purposes*: Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection and Subcomm. on Communications, Technology, and the Internet of the H. Comm. on Energy and Commerce, 111th Cong. 3 (2010) (statement of Lori Faith Cranor).

61,022 in 2016.[22] AT&T received 15,913 demands for real-time data from July 2017 to June 2018, as well as 26,214 "exigent" requests, which likely included requests for real-time data.[23] T-Mobile received an astounding 46,395 requests for "prospective," i.e., real-time, location data in 2017.[24]

ARGUMENT

Government cell phone tracking "achieves near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user." *Carpenter*, 138 S. Ct. at 2218. Few individuals are exempt; the U.S. has more cell phones than people.[25] No time is off limits; people keep their phones with them and turned on nearly all the time. And no haven is safe; this surveillance penetrates homes, doctors' offices, religious sanctuaries, and private political

---

[22] Sprint, *Sprint Corporation Transparency Report – January 2018* at 3-4 (Jan. 2018), *at* http://goodworks.sprint.com/content/1022/files/Transparency%20Report%20January%202018.pdf (including court orders and emergency requests); Sprint, *Sprint Corporation Transparency Report – August 2017* at 3-4 (Aug. 2017), http://goodworks.sprint.com/content/1022/files/Transparency%20Report%20July%202017.pdf.

[23] *See* AT&T, *AT&T Transparency Report* (last visited Aug. 18, 2018), *at* http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html.

[24] T-Mobile US, Inc., *Transparency Report for 2017* (2018), *available at* https://www.t-mobile.com/content/dam/t-mobile/corporate/media-library/public/documents/TransparencyReport2017.pdf.

[25] *Carpenter*, 138 S. Ct. at 2211.

gatherings. Yet the Commonwealth advances the sweeping assertion that this surveillance can be undertaken in real time, for any person, without a warrant. Comm. Br. 13-14.

This assertion should be rejected. Courts have consistently ensured that technological advances do not undermine core privacy protections. *See, e.g.*, *Augustine*, 467 Mass. at 245-46; *Carpenter*, 138 S. Ct. at 2216-19. Viewed in that light, this case is straightforward. If police officers warrantlessly enter a private home to determine a defendant's location, they cannot successfully justify that invasion of privacy by arguing that they stayed inside for just a short time. Here, law enforcement warrantlessly used a person's cell phone to generate precise real-time information that placed him inside a home, so the result should be no different.

I. The Commonwealth's warrantless acquisition of Mr. Almonor's real-time location coordinates invaded his privacy interests protected by art. 14 and the Fourth Amendment.

The Superior Court held that the Commonwealth conducted a "search" when it obtained precise real-time location information for Mr. Almonor's phone, and that the Commonwealth's failure to obtain a warrant for that search violated art. 14 and the Fourth Amendment. RA 85. The court recognized that, even though the data covered only a short period of time,

"it is not . . . the length of the monitoring that offends the constitution but rather the *place* of the monitoring" — here, inside a home — "that does." RA 83. That decision is correct.

A. The Constitution protects location information derived from a cell phone.

Decisions by this Court, the U.S. Supreme Court, and other state supreme courts support the conclusion that the Commonwealth must get a warrant before demanding precise real-time cell phone location information from a cell phone carrier. In *Augustine*, this Court recognized that art. protects an individual's privacy interests in location information about her phone, and that the Commonwealth conducts a search for purposes of art. 14 when it obtains such information. *Augustine*, 467 Mass. at 254. Subsequently, this Court held that acquiring less than six hours' worth of historical telephone-call CSLI is not a search. *Estabrook*, 472 Mass. at 854.

After the parties briefed this appeal, the U.S. Supreme Court held the federal government violated the Fourth Amendment when it warrantlessly requested, via two different court orders, 152 and seven days' worth of a suspect's cell site location information. *Carpenter*, 138 S. Ct. at 2212. Consistent with *Augustine*, the *Carpenter* decision recognized that the government invades the reasonable privacy interests of

a cell phone's owner when it acquires historical CSLI; it declined to apply the third-party doctrine to CSLI; and it held that a search of historical CSLI covering more than a limited period constitutes a search that must be supported by probable cause warrant to comply with the Fourth Amendment. *Id.* at 2217-23.

Like *Augustine*, *Carpenter* did not expressly address real-time cell phone tracking. *Id.* at 2220. Unlike *Augustine* and *Estabrook*, the Carpenter decision expressly did *not* address whether acquiring such information for a relatively short duration would be exempt from the warrant requirement. *Id.* at 2217 n.3.[26] Nonetheless, several aspects of *Carpenter*'s analysis suggest that obtaining real-time coordinates from a cell phone for even one data point is a search subject to the warrant requirement of art. 14 and the Fourth Amendment.

First, *Carpenter* began by reiterating the need for vigilance to safeguard accepted privacy interests from being eroded by evolving technologies. "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive

[26] At oral argument, Chief Justice Roberts expressed skepticism about a duration-based rule like the one in *Estabrook*. *See* Oral Argument Tr. at 11-12, *Carpenter v. United States*, No. 16-402 (U.S. Nov. 29, 2017), *at* https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_3f14.pdf.

eyes," the Court explained, "this Court has sought to 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was passed." 138 S. Ct. at 2214. These concerns are also paramount here. There was no analogue to real-time cell phone GPS pings, or anything even approximating their capacity to locate anyone, anywhere, at any time, when the Massachusetts Declaration of Rights was passed. *Cf. United States v. Jones*, 565 U.S. 400, 421 n.3 (2012) (Alito, J., concurring) (noting, in relation to automobile GPS, the implausibility of "a very tiny constable" concealing himself in a stagecoach).

Second, *Carpenter* emphasized that CSLI searches can reach beyond areas amenable to traditional surveillance:

> Unlike the bugged container in [*United States v. Knotts*, 460 U.S. 276 (1983)], or the car in *Jones*, a cell phone — almost a "feature of human anatomy" - tracks nearly exactly the movements of its owners. While individuals regularly leave their vehicles, they compulsively carry cell phones with them at all times. A cell phone faithfully follows its owner beyond public thoroughfares into private residences, doctor's offices, political headquarters, and other potentially revealing locales.

138 S. Ct. at 2218 (internal citations omitted). This reasoning also applies to real-time phone location

tracking, because it, too, allows the government to follow people into homes and other private spaces.

Third, *Carpenter* explained that cell phone tracking allows the government to track essentially any person at any time. "[T]his newfound tracking capacity runs against everyone," the Court wrote, and "[o]nly the few without cell phones could escape this tireless and absolute surveillance." *Id.*

Although the Court noted the "retrospective quality" of historical CSLI, *id.*, its concerns about "tracking capacity [that] runs against everyone" apply fully to real-time location tracking at the direction of law enforcement, even when that tracking is for a short duration. The police simply cannot, through traditional measures or resources, instantly locate any person at any time. Before cell phones, police could "visually track a suspect from some starting location, and electronic tracking devices . . . [like beepers and GPS devices] have augmented this preexisting capacity." *Jones v. United States*, 168 A.3d 703, 712 (D.C. 2017). But that kind of tracking required having at least one officer physically find the suspect, in order to begin visual surveillance or install a tracking device. *Id.* For people in public spaces, the government lacked the personnel to track

everyone. For people in private spaces, finding them might not be possible.[27]

Not so with real-time cell phone tracking. Today police can locate a person without knowing in advance where or even who they are, by "remotely activat[ing] the latent tracking function of a device that the person is almost certainly carrying in his or her pocket or purse: a cellphone." *Id.* Police can pluck a suspect's precise location out of thin air, with no more information than that person's cell phone number. See *Tracey v. State*, 152 So. 3d 504, 525 (Fla. 2014) ("Officers learned of [Tracey's] location on the public roads, and ultimately inside a residence, only by virtue of tracking his real time cell site location information emanating from his cell phone."). The government's power "not merely to track a person but to locate him or her" cheaply, easily, and precisely violates expectations of privacy by providing police with an unprecedented capability which, without regulation, is prone to abuse. *Jones*, 168 A.3d at 712.

Fourth, the Supreme Court was not persuaded that these privacy interests are diminished by the argument that cell phone users voluntarily expose their

[27] Tracking a person from a public into a private space, while possible if the police knows where the person was to begin with, requires a warrant. *United States v. Karo*, 468 U.S. 705, 715 (1984).

location data, or by the argument, which the Commonwealth repeats here, that location data can be imprecise. *See* Comm. Br. 16, 21. The Court explained that "[c]ell phone location information is not truly 'shared' as one normally understands the term," because the services available on cell phones make them "indispensable to participation in modern society," and because "a cell phone logs a cell-site record by dint of its operation." *Carpenter*, 138 S. Ct. at 2220 (internal citations omitted). For real-time location tracking, the absence of any meaningful disclosure of location by the cell phone user is even more pronounced. The user does nothing besides have a phone that is turned on; the ping is accomplished entirely by the government or its agent. Likewise, *Carpenter* recognized that technological advances will make this data more precise over time. *Id.* at 2218-19; *accord Augustine,* 467 Mass. at 254. Those advances are on full display here; the Commonwealth obtained coordinates that specifically identified the home where Mr. Almonor was found. RA 64.

For all these reasons, *Carpenter*'s reasoning indicates that the Commonwealth's acquisition of precise cell phone location information to track a person in real time, whether for a relatively short duration or not, constitutes a search under art. 14 and the Fourth Amendment. Moreover, two other state

supreme courts already have held that real-time cell phone tracking is a search, irrespective of duration. *Tracey*, 152 So. 3d at 525-26 (interpreting the Fourth Amendment); *State v. Earls*, 70 A.3d 630, 644 (N.J. 2013) (interpreting the New Jersey constitution).

B. The distinctive characteristics of real-time location data justify recognizing a privacy interest that is not limited by time.

Citing this Court's prior holding that law enforcement can warrantlessly acquire less than six hours of historical telephone-call CSLI, the Commonwealth argues that no search occurred here because it acquired less than six hours of GPS data. *See* Comm. Br. 18; *Estabrook*, 472 Mass. at 858. This argument should be rejected. On its face, *Estabrook*'s six-hour carve-out does not apply to real-time tracking, *id.* at 858 & n.12, and compelling reasons show that it should not be extended here.

First, real-time tracking allows the Commonwealth to determine exactly where a person is — in the moment — even if it previously had no way of knowing the individual's location and so had no ability to find or track that person using traditional surveillance techniques. *See Tracey*, 152 So. 3d at 523. Second, real-time tracking reveals otherwise-protected information such as whether a person is in a private space. And each of these intrusions is especially

acute where, as here, the Commonwealth obtains real-time data by requiring the carrier "to create particular prospective [location data] that it otherwise would not have created." *Commonwealth v. Fredericq*, 93 Mass. App. Ct. 19, 28 (2018), *further appellate review allowed* (Mass. July 30, 2018) (No. FAR-26004).

1. An individual has two separate but related privacy interests in her real-time location.

The privacy interests at issue in this case may be even stronger than the interests in historical location information recognized in *Augustine* and *Carpenter*.[28] This is because real-time location data impacts privacy interests in both one's physical location in the moment and one's movements over time. *See Maryland Real-Time Order*, 849 F. Supp. 2d at 538.

The *Maryland Real-Time Order* case is instructive on this point. In addressing real-time tracking, the court held that the government's acquisition of real-time CLSI implicated each of these two interests

[28] *See, e.g.*, *Maryland Real-Time Order*, 849 F. Supp. 2d at 538 (holding that the government's "request for real-time location data implicates . . . the subject's right to privacy in his location"); *United States v. Ellis*, 270 F. Supp. 3d 1134, 1145-46 (N.D. Cal. 2017) (holding that "cell phone users have an even stronger privacy interest in real time location information associated with their cell phones, which act as a close proxy to one's actual physical location because most cell phone users keep their phones on their person or within reach").

separately, and was therefore a search for purposes of the Fourth Amendment. *Id.* This distinction between location and movement is significant, because it crystalizes that — wholly apart from their movements over time — people have protected privacy interests in their real-time location at any given moment. That is Mr. Almonor's interest here. Under the logic of *Maryland Real-Time Order*, no further action by the Commonwealth beyond obtaining real-time location data at one moment of time was necessary for its actions to invade Mr. Almonor's protected interest in his location and, thus, to constitute a search under art. 14 and the Fourth Amendment.

2. Real-time cell phone tracking, even for a brief period, is likely to invade constitutionally-protected space.

The Commonwealth's ability to ping a cell phone's GPS whenever the phone is on means that the Commonwealth can acquire precise location information whenever a cell phone user is in a constitutionally-protected space. This capability cuts strongly against affording the Commonwealth a license to warrantlessly obtain even one moment of precise real-time location information.

Precisely because real-time tracking can implicate protected spaces, the Supreme Court and lower courts have long recognized that the scope of an

individual's privacy interest in his or her real-time location can include protection against short-duration searches. In *Karo*, the Supreme Court considered monitoring conducted by the use of a beeper installed in a can of ether to determine that the ether was present in a private home. *United States v. Karo*, 468 U.S. 705 (1984). The government obtained data from the beeper only briefly, at two times in the same day. *Id.* at 714. Yet the Court held that "the monitoring of [the] beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment." *Id.* The Court drew an analogy to physical entry, noting that if law enforcement had entered the residence surreptitiously "to verify that the ether was actually in the house . . . , there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment." *Id.* at 715.

The Court therefore rejected the government's argument that it should be free, without a warrant, to use "an electronic device" to determine "whether a particular article — or a person, for that matter — is in an individual's home at a particular time." *Id.* at 716. For purposes of what amounts to a search, there is no meaningful difference between the conduct in *Karo* and the Commonwealth's acquisition of real-time GPS coordinates for one point in time to determine

someone's "Precision Location." RA 68. Both are a search.

Similarly, in *Kyllo*, the Supreme Court addressed the use of thermal imaging technology to scan the defendant's home for heat signals that could indicate use of lamps to grow marijuana. *Kyllo v. United States*, 533 U.S. 27 (2001). The scan "took only a few minutes." *Id.* at 30. Yet the Court held that the scan constituted a search because it involved "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally-protected area." *Id.* at 34. The Court explicitly rejected arguments that the police had not obtained "enough" information to count as an invasion of the protected privacy interest: "The Fourth Amendment's protection of the home has never been tied to measurement of the quality *or quantity* of information obtained." *Id.* at 37 (internal citations omitted) (emphasis added).

Again, the issue in *Kyllo* resembles the issue here. The Commonwealth's ability to ping a cell phone whenever it is turned on, and to use that ping to generate a latitude and longitude that reveal the cell phone user's "Precision Location," RA 68, means that real-time precision tracking will disclose an individual's location when he or she is in a

constitutionally-protected space, whether it is a medical office, religious space, or a private home.

It makes no difference that, in *Kyllo*, the police knew they were obtaining information from inside a private home, while with real-time tracking the police do not necessarily know in advance whether the location revealed will be public or private. Both the Supreme Court and this Court have expressly rejected this argument. *See Karo*, 468 U.S. at 718; *Augustine*, 467 Mass. at 253. Thus, regardless of the "quantity of information obtained" — be it for one moment or one month — obtaining real-time GPS coordinates amounts to a search. *Kyllo*, 533 U.S. at 37.

Without citing *Karo* and *Kyllo*, the Commonwealth relies on cases involving surveillance of vehicles in *public*. *See* Comm. Br. 19. In *Rousseau*, which addressed the Commonwealth's monitoring of a car using a GPS tracking device, the Court 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." *Commonwealth v. Rousseau*, 465 Mass. 372, 382 (2013). While the Court noted that the surveillance had spanned 31 days, it emphasized that the surveillance involved the "comings and goings *in public places.*" *Id.* (emphasis added). Similarly, although the extent

of the GPS monitoring informed the concurring opinions in *Jones*, that too was a case about "monitor[ing] [a] vehicle's movements on public streets." *Jones*, 565 U.S. at 402 (opinion of the Court); *cf. id.* at 415 (Sotomayor, J., concurring); *id.* at 429-30 (Alito, J., concurring).

Tracking a car on public streets is far less likely to intrude on a constitutionally-protected space than tracking a cell phone in real time.[29] *Any* one ping of a cell phone can reveal someone's location in a private space, which is exactly what happened here. RA 64-65. This is because individuals and their cell phones go places that automobiles cannot go. For example, an automobile GPS may track a car to a parking garage in a busy city, but it reveals nothing about the location(s) the driver visits after leaving the vehicle, including private offices, friends' apartments, or even their own home. Further, unlike with GPS tracking a car on a public road, the Commonwealth could not obtain information about an individual's location in a private space through traditional surveillance without conducting a search.

[29] In *Augustine*, Justice Gants made this point with respect to registration CSLI compared to telephone-call CSLI, and it applies with the same force here. *Augustine*, 467 Mass. at 263 (Gants, J., dissenting).

Therefore, because the government engages in a search whenever it physically intrudes on protected spaces to obtain information, *see Jones*, 565 U.S. at 406 n.3, and because obtaining precise real-time cellphone location data acutely risks revealing an individual's location in a protected private space, the Commonwealth conducts a search under art. 14 and the Fourth Amendment when it obtains any cell phone GPS coordinates, regardless of duration. The Court should therefore decline to apply an *Estabrook*-type durational rule to the privacy interest at issue here.

C. A contrary rule would unduly burden cell phone users and lead to perverse results.

Under the Commonwealth's approach, individuals would face an impossible choice: either reject owning a cell phone, keep it turned off virtually all the time, or subject yourself to warrantless government monitoring at six-hour intervals of the government's choosing. But this is no choice at all. As this Court and the Supreme Court have recognized, carrying a cell phone is "'an indispensable part of modern [American] life.'" *Augustine*, 467 Mass. at 245 (quoting *Earls*, 214 N.J. at 586); *see also Carpenter*, 138 S. Ct. at 2220. Article 14 and the Fourth Amendment exist precisely to protect the privacy interests of people when they are within society, not to require them to opt out of participating in society.

Nor it is viable to require individuals to turn off their phones to avoid real-time tracking. "Requiring a cell phone user to turn off the cell phone just to assure privacy from governmental intrusion . . . places an unreasonable burden on the user to forego necessary use of his cell phone, a device now considered essential by much of the populace." *Tracey*, 152 So.3d at 523. It is easy to imagine vitally important reasons why people cannot turn off their phones to avoid being tracked:

- Parents at home while their children are at the movies, or a school dance;
- Individuals waiting for a doctor to call with the results of medical tests;
- Employees who need to be available to employers or clients; or
- Therapists or counselors or clergy who need to be on call for emergencies.

In each of these situations, the act of simply being available to others would render individuals susceptible to surveillance through real-time tracking. Article 14 and the Fourth Amendment cannot properly be read to mandate isolationism as a condition of preserving privacy.

Beyond creating unreasonable demands on cell phone users, the Commonwealth's proposal would create perverse incentives for law enforcement. The

Commonwealth's position would encourage the police to use real-time cell phone tracking to obtain what they could not through traditional surveillance. For example, under the Commonwealth's rule, officers still could not warrantlessly enter a house for even one minute just to check whether a suspect is inside. *See Karo*, 468 U.S. at 715. But they could warrantlessly use the suspect's cell phone to track him inside that same house for up to six hours. This rule would offer individuals no protected privacy interest in their current location at any given moment, even when they are in private spaces, a result that cannot be squared with longstanding constitutional norms and widespread public expectations. Bedrock privacy protections should not be subject to such facile circumvention by technological measures.

II. The Commonwealth's warrantless demand for the creation of real-time location coordinates invaded property interests protected by art. 14 and the Fourth Amendment.

A "property-based" approach supplies a separate and independent basis for affirming the judgment below. *Jones*, 565 U.S. at 405. That approach, like the privacy-based approach discussed above, yields the conclusion that the Commonwealth's warrantless acquisition of precise real-time location information about Mr. Almonor's phone violated art. 14 and the Fourth Amendment.[30]

A. Precedents from this Court and the U.S. Supreme Court support a property-based approach to real-time cell phone tracking.

Article 14 of the Massachusetts Declaration of Rights protects against "unreasonable searches, and seizures, of [someone's] person, his houses, his papers, and all his possessions." Similarly, the Fourth Amendment to the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In *Carpenter*, Justice Gorsuch suggested that deciding what constitutes a search or seizure of CSLI should be determined with reference to "positive legal rights," such as property interest — in other words, by asking

[30] The Court may affirm on this alternate ground. *Commonwealth v. Va Meng Jo*, 425 Mass. 99, 100 (1997).

whether what the government obtained "was *yours* under law." *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting). On this view, "a person's cell-site data could qualify as *his* papers or effects" under the Fourth Amendment, i*d.* at 2272, or her papers or possessions under art. 14.

This view fits squarely within settled precedent on both art. 14 and the Fourth Amendment. In *Connolly*, this Court held that the police had undertaken art. 14 seizures when they installed a GPS device on the defendant's minivan and then used that device to track the minivan's (and thus the defendant's) location. *Connolly*, 454 Mass. at 810. The Court held that one seizure occurred when police installed the GPS device, which involved entering the minivan and "operat[ing] . . . [its] electrical system," and that another seizure occurred when "the police use[d] the defendant's minivan to conduct GPS monitoring for their own purposes." *Id*. at 822-23. The Court emphasized that, by using the minivan, "the police asserted control over it, converting the minivan to their own use notwithstanding the defendant's continued possession." *Id.* at 823.

Supreme Court cases have reached similar conclusions, while characterizing the infringement as a "search" rather than a "seizure." In *Jones*, the Court held that the government conducted a search by

"install[ing]" a GPS device on a target's vehicle, and "us[ing] . . . that device to monitor the vehicle's movements." 565 U.S. at 404. The Court reasoned that attaching the GPS device to the defendant's car was a common-law trespass to chattels, *id.* at 405, 426, that "encroached on a protected area" because a vehicle is an "effect" under the Fourth Amendment. *Id.* at 404, 410. The Supreme Court has also held that the government conducts a search "when it attaches a [GPS monitor] to a person's body, without consent, for the purpose of tracking that individual's movements," *Grady v. North Carolina*, 135 S. Ct. 1368, 1370 (2015) (per curiam), and when it "physically intrudes on the curtilage [of a home] to gather evidence." *Collins v. Virginia*, 138 S. Ct. 1663, 1670 (2018) (citing *Jardines*, 569 U.S. at 11).

Together, these cases indicate that the government undertakes a search or seizure when it "operat[es]," *Connolly*, 454 Mass. at 822, "use[s]," *Jones*, 565 U.S. at 402, or "physically intrud[es] on" persons, houses, papers, effects, or possessions within the meaning of art. 14 or the Fourth Amendment. *Florida v. Jardines*, 569 U.S. 1, 5 (2013) (internal quotation marks omitted).

B. The Commonwealth's warrantless acquisition of precise real-time location information intruded on Mr. Almonor's person, papers, effects, and possessions.

The Commonwealth found Mr. Almonor by turning his cell phone, and with it his body, into a beacon that broadcast his precise location to the Commonwealth. This conduct interfered with the security of Mr. Almonor's person, papers, effects, and possessions.

First, the Commonwealth interfered with Mr. Almonor's effects and possessions because it commandeered his phone, and indeed directed the "operation of [its] electrical system." *Connolly*, 454 Mass. at 822. Notwithstanding Mr. Almonor's property interest in using his cell phone exclusively for his own purposes, the Commonwealth demanded that Sprint use it to generate "Precision Location" data. RA 68. To carry out that demand, Sprint apparently caused Mr. Almonor's phone to send a signal — unbeknownst to Mr. Almonor — allowing the Commonwealth to locate him. RA 64-65, 68, 72-73; *see also* Almonor Br. 12. "[C]ell phones are 'effects' as that term is used in the Fourth Amendment," *Tracey*, 152 So. 3d at 524, and necessarily "possessions" as that term is used in art. 14. The Commonwealth's warrantless operation of Mr. Almonor's cell phone therefore violated art. 14 and the Fourth Amendment.

Second, the Commonwealth interfered with Mr. Almonor's person because, by operating his phone, the Commonwealth in effect installed a tracking device on Mr. Almonor himself. Just as the officers installed

the GPS devices in *Connolly* and *Jones* so they could "use the defendant's [vehicle] to conduct GPS monitoring for their own purposes," *Connolly*, 454 Mass. at 822-23, here the Commonwealth operated Mr. Almonor's phone so it could use his *body* to conduct GPS monitoring for its own purposes. *See also Grady*, 135 S. Ct. at 1370. The Commonwealth likely caused Sprint to "ping" Mr. Almonor's phone precisely because the Commonwealth expected the phone to be attached to Mr. Almonor's person. This action violated art. 14 and the Fourth Amendment.

Finally, by causing Sprint to generate precise real-time location data about him, the Commonwealth interfered with the security of Mr. Almonor's papers. The federal Telecommunications Act requires "express prior authorization of the customer" before a service provider can "use or disclose . . . call location information." 47 U.S.C. § 222(f). In *Carpenter*, Justice Gorsuch suggested that location information in the hands of a third party can fall under the Fourth Amendment's protection of a person's "papers" even when those records are the third party's business records. 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting). Here, there is no evidence that the location information at issue was created as a business record; it appears to have been created at the Commonwealth's insistence. On this record, Mr.

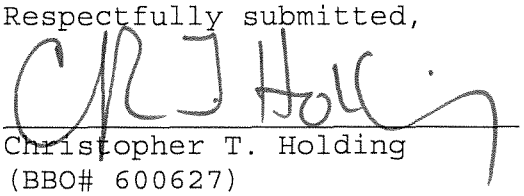
Almonor had a property right in that information, and the Commonwealth's warrantless acquisition of it violated art. 14 and the Fourth Amendment.

CONCLUSION

When the Commonwealth obtains precise real-time cellphone location information, whether it covers a relatively short period or a longer one, it engages in a search under art. 14 and the Fourth Amendment. And when the Commonwealth requires a cell phone carrier to create that information, it also infringes property interests protected by art. 14 and the Fourth Amendment. Applying either standard here, the Court should affirm the decision below.

Dated: August 20, 2018

Respectfully submitted,



Christopher T. Holding
(BBO# 600627)
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, MA 02210
Tel.: 617.570.1000
Fax.: 617.523.1231
CHolding@goodwinlaw.com

Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: 415-436-9333
jlynch@eff.org

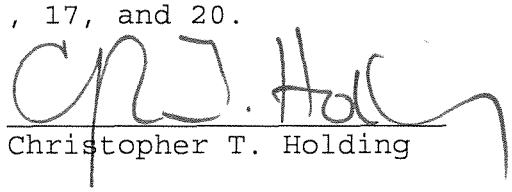
Chauncey B. Wood
(BBO# 600354)
WOOD & NATHANSON, LLP
50 Congress Street,
Ste. 600
Boston, MA 02109
Tel.: 617.776.1851
cwoodesq@gmail.com

Matthew R. Segal
(BBO# 654489)
Jessie J. Rossman
(BBO# 670685)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS, INC.
211 Congress Street
Boston, MA 02110
Tel: 617-482-3170
msegal@aclum.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 16(k) of the of the Massachusetts Rules of Appellate Procedure, the undersigned counsel states that this brief complies with the applicable rules of court that pertain to the filing of briefs, including but not limited to Mass. R. App. P. 16(e), 16(f), 16(h), 17, and 20.



Christopher T. Holding

CERTIFICATE OF SERVICE

I, Christopher T. Holding, hereby certify that on August 20, 2018, I caused two copies of the foregoing Brief Amici Curiae by the Electronic Frontier Foundation, the America Civil Liberties Union of Massachusetts, Inc. , and the Massachusetts Association of Criminal Defense Lawyers to be delivered via first-class U.S. Mail, postage prepaid, to each party separately represented as identified below:

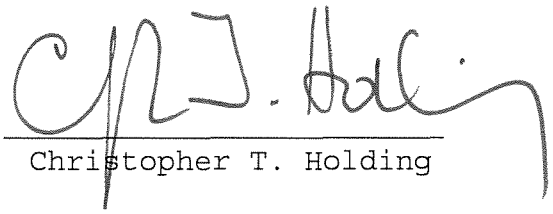
Nathaniel Kennedy
Office of the District Attorney, Plymouth County
166 Main Street
Brockton, MA 02301

Counsel for the Commonwealth

Matthew Spurlock
Committee for Public Counsel Services
44 Bromfield Street
Boston, MA 02108

Randall K. Power
Law Office of Randall K. Power
400 Trade Center, Suite 5900
Woburn, MA 01801

Counsel for Defendant-Appellee



Christopher T. Holding