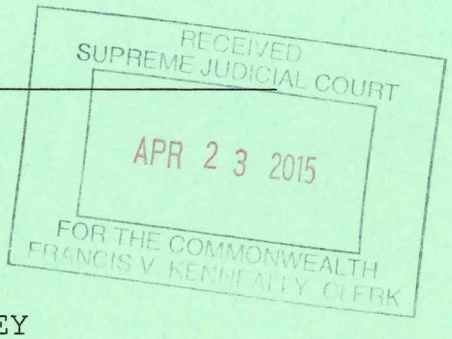
COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

No. SJC-11833



COMMONWEALTH
Appellee

v.

JASON ESTABROOK & ADAM BRADLEY
Appellants

ON APPEAL FROM AN ORDER OF THE
MIDDLESEX SUPERIOR COURT

BRIEF FOR AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF THE APPELLANTS

CYBERLAW CLINIC
HARVARD LAW SCHOOL
BERKMAN CENTER FOR INTERNET & SOCIETY

Andrew Sellars (BBO#682690)
23 Everett Street, 2nd Fl.
Cambridge, MA 02138
Tel: (617) 495-7547
Fax: (617) 495-7641
asellars@cyber.law.harvard.edu

On the brief:

Matthew R. Segal (BBO#654489)
msegal@aclum.org
Jessie J. Rossman (BBO#670685)
jrossman@aclum.org
AMERICAN CIVIL LIBERTIES UNION
OF MASSACHUSETTS FOUNDATION
211 Congress Street
Boston, MA 02110
Tel: (617) 482-3170
Fax: (617) 451-0009

Hanni M. Fakhoury
hanni@eff.org
Andrew Crocker
andrew@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993

Vivek Krishnamurthy
vkrishnamurthy@cyber.law.harvard.edu
CYBERLAW CLINIC
HARVARD LAW SCHOOL
BERKMAN CENTER FOR INTERNET & SOCIETY
23 Everett Street, 2nd Fl.
Cambridge, MA 02138
Tel: (617) 495-7547
Fax: (617) 495-7641

INTEREST OF THE AMICI CURIAE

The American Civil Liberties Union of Massachusetts ("ACLUM"), an affiliate of the national American Civil Liberties Union, 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. Among the rights that ACLUM defends through direct representation and amicus briefs is the right to be free from unreasonable searches and seizures. See, e.g., *Commonwealth* v. *Augustine*, 467 Mass 230 (2014); *Commonwealth* v. *Rousseau*, 465 Mass 372 (2013). Accordingly, ACLUM has an interest in this case because it could significantly impact constitutional protections against unreasonable government access to cell phone location data.

The Electronic Frontier Foundation ("EFF") is a member-supported civil liberties organization based in San Francisco, California that works to protect innovation, free speech, and privacy in the digital world. With over 25,000 active donors, EFF represents the interests of technology users both in court cases and in broader policy debates surrounding the application of law in the digital age. As part of its mission, EFF has served as *amicus curiae* in landmark state and federal cases addressing Fourth Amendment

issues raised by emerging technologies, including location-based tracking technologies like GPS and cell-site tracking. See, e.g., *Commonwealth* v. *Rousseau*, 465 Mass 372 (2013); *Commonwealth* v. *Augustine*, 467 Mass. 230 (2014); *Riley* v. *California*, 134 S. Ct. 2473 (2014); *United States* v. *Jones*, 132 S. Ct. 945 (2012); *United States* v. *Davis*, 754 F.3d 1205, *rehearing en banc granted,* 573 F. App'x 925 (11th Cir. 2014); *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).

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Massachusetts Cases

Federal Cases

State Cases

Federal Statutes

State Statutes

Massachusetts Constitutional Provisions

Federal Constitutional Provisions

Other Authorities

SUMMARY OF ARGUMENT

This Court has held that when the Commonwealth obtains two weeks' worth of someone's cell site location information (CSLI), it conducts a "search" for which a warrant is required under Article 14 of the Massachusetts Declaration of Rights. *Commonwealth* v. *Augustine*, 467 Mass. 230 (2014). This case asks the Court to decide whether the Commonwealth can avoid *Augustine*'s warrant requirement if, after obtaining two weeks of CSLI without a warrant, the Commonwealth later claims that it is truly interested in only a six-hour portion covering a "critical time period," thereby excusing its failure to comply with *Augustine*. RA 31. The answer is clear: they cannot. The warrant requirement applies fully in this circumstance.

As a threshold matter, *Augustine* unequivocally establishes that when the Commonwealth warrantlessly obtains two weeks of CSLI, it violates Article 14 of the Massachusetts Declaration of Rights ("Article 14"). This is true no matter how much CSLI the Commonwealth ultimately uses. Under fundamental constitutional principles, it is the initial intrusion into an individual's expectation of privacy that triggers the constitutional offense. *United States* v. *Calandra*, 414 U.S. 338, 354 (1974). Although *Augustine*

indicated that the Commonwealth might be able to avoid a warrant requirement by narrowing its "request" to a six-hour period, 467 Mass. at 255 n.37, neither *Augustine* nor any other cases suggest that an overbroad and unconstitutional request may be salvaged by the Commonwealth's after-the-fact pronouncement that it is not interested in all of the CSLI it unlawfully obtained.

This case involves a two-week request that is squarely controlled by *Augustine*. The Superior Court's flawed reasoning, however, also provides an opportunity to emphasize that a specific temporal exception is not necessary to protect public safety. Long-recognized exceptions to the warrant requirement — such as exigent circumstances — allow the Commonwealth to access limited amounts of CSLI without a warrant in appropriate cases. States across the country have continued to rely on such traditional exceptions rather than create a specific temporal exception for CSLI requests.

Finally, this is an appropriate case to revisit the notion that "there is some period of time for which the Commonwealth may [warrantlessly] obtain a person's historical CSLI . . . because the duration is too brief to implicate the person's reasonable privacy interest." *Augustine*, 467 Mass. at 255. The highly

revealing nature of even small amounts of CSLI and the difficulty courts have had in administering a temporal exception both point to the need for a bright-line warrant requirement whenever the Commonwealth seeks to obtain CSLI.

ARGUMENT

I. Warrantlessly Obtaining Two Weeks of CSLI Violates Article 14, No Matter How Much of That CSLI the Commonwealth Ultimately Uses.

In *Augustine*, this Court held that "the warrant requirement of article 14 applies" where the Commonwealth obtains CSLI "cover[ing] a two-week period." 467 Mass. at 232. The Court explained that even "assum[ing] that a [comparable] request for historical CSLI" would not require a warrant if the request were "for a period of six hours or less," a two-week request requires a warrant because "tracking" someone's movements "for two weeks" is "more than sufficient to intrude upon [an] expectation of privacy . . . ." *Id.* at 254-255, 255 n.37.

In this case, the Commonwealth again obtained CSLI covering a two-week period. RA 3. Nevertheless, the Superior Court determined that *Augustine*'s holding did *not* govern. RA 31-32. Instead, it reasoned that the defendants lacked a reasonable expectation of privacy in the CSLI pertaining to "the approximately

six hours surrounding the time of the murder," and that a "warrant was not required" for that portion of CSLI. RA 31-32.

This reasoning is fatally flawed. It contradicts fundamental constitutional principles, under which intrusions on privacy are evaluated based on the extent of the governmental intrusion, not the extent to which the government ultimately uses the information obtained from that intrusion. It also contradicts, and in fact threatens to eviscerate, this Court's holding in *Augustine*. Under this theory, the Commonwealth could warrantlessly *obtain* two weeks of CSLI – or two years, or two decades - so long as it ultimately wants to *use* only six hours or less. This Court should reaffirm that where, as here, the Commonwealth warrantlessly obtains two weeks of CSLI, no portion of that location information has been lawfully obtained.

A. The Ruling Below Contradicts Longstanding Constitutional Principles.

The Fourth Amendment and Article 14 protect against unreasonable governmental searches. Because these provisions protect an individual's reasonable expectation of privacy, the initial intrusion itself triggers the constitutional offense. Cf. *United States* v. *Calandra*, 414 U.S. at 354 (1974) ("The purpose of

the Fourth Amendment is to prevent unreasonable government intrusions [and] unjustified governmental invasions [of privacy.]"). As the Supreme Court recognized in *United States* v. *Balsys*, it is "commonsense that breaches of privacy are complete at the moment of illicit intrusion, whatever use may or may not later be made of their fruits." 524 U.S. 666, 692 (1998). A violation of the constitutional protection against unreasonable searches is therefore "fully accomplished at the time of the unreasonable government intrusion" irrespective of "whether or not the evidence is sought to be used in a criminal trial." *United States* v. *Verdugo-Urquidez*, 494 U.S. 259, 264 (1990).

B. The Ruling Below Contradicts *Augustine*.

Consistent with these longstanding principles, *Augustine* determined that it is the Commonwealth's collection of location information, not its subsequent use, which triggers Article 14 protection. Under this holding, *Augustine* squarely foreclosed the view that the Commonwealth can warrantlessly seek and obtain two weeks of CSLI without violating Article 14. This Court was unequivocal: "the warrant requirement of art. 14 applies" if "the CSLI *obtained* covered a two-week period." 467 Mass. at 232 (emphasis added); see also

id. at 255 (holding that "the government-compelled production of [] CSLI records . . . constituted a search in the constitutional sense to which the warrant requirement of art. 14 applied").

Although *Augustine* also stated that the duration of CSLI "*sought*" or "*request[ed]*" would likely bear on "the reasonable expectation of privacy calculus," it nowhere suggested that periods of CSLI sought or requested by the Commonwealth can be excluded from that calculus if they are later deemed non-critical to a criminal case. 467 Mass. at 254-255, 255 n.37 (emphasis added). This Court did not write that a request for two weeks of historical CSLI does not require a warrant so long as the Commonwealth is truly *interested* in or ultimately *uses* only six hours or less. Rather, it wrote that it would be "reasonable to assume that a *request* for historical CSLI . . . for a period of six hours or less would not require the police to obtain a search warrant." *Id.* at 255 n.37 (emphasis added).[1]

[1] Had this Court actually adopted the Superior Court's reasoning in *Augustine*, it could have allowed the Commonwealth to utilize the CSLI obtained from "the most critical time period" without a warrant. RA 31. Its rejection of that rule and decision to instead require probable cause to support the entire request further contradicts the Superior Court's analysis.

The Superior Court misapprehended this holding. It acknowledged that the Commonwealth sought and obtained two weeks of CSLI without a warrant and without probable cause.[2] Yet, in applying Article 14, the court focused on whether the defendants had a reasonable expectation of privacy in six hours of CSLI immediately before and after the murder. RA 31-33. The Commonwealth did not "request" six hours of CSLI, however; it requested two weeks. Compare RA 3, with *Augustine*, 467 Mass. at 255 n.37. Because the constitutional violation is triggered by the collection of information, the proper question is whether the defendant had a reasonable expectation of privacy in two weeks of information (which *Augustine* clearly holds he does), not six hours. See *Augustine*, 467 Mass. at 254-55. The decision to nevertheless seek this information without a warrant "fully accomplished" the Article 14 violation. *Verdugo-Urquidez*, 494 U.S. at 264 (1990).

Adopting the Superior Court's reasoning would frustrate, rather than further, *Augustine*'s holding. Under the Superior Court's analysis, the Commonwealth

[2] The Superior Court held that "it is clear that [the § 2703(d)] applications do not meet the probable cause standard." RA 31.

could obtain weeks, months or even years of CSLI without a warrant, so long as it only ultimately used six hours. But this broad collection would raise the same privacy concerns that were dispositive in *Augustine*. 467 Mass. at 247-249; see also *United States* v. *Jones*, 132 S. Ct. 945, 956 (2012)(Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").

From a constitutional perspective, the time to narrow a request is before that request is made – when the privacy concerns can still be protected - not after. Cf. *Commonwealth* v. *Valerio*, 449 Mass 562, 567 (2007) (noting that one of the purposes of the warrant requirement is "to protect individuals from general searches"). The Superior Court's analysis contradicts *Augustine* and perversely incentivizes the Commonwealth to "search first, narrow later," even if the Commonwealth could have focused its request from the start.[3] To avoid this outcome and uphold the clear

[3] Indeed, that is exactly what happened here. The Commonwealth requested two weeks of CSLI even though "the police investigation revealed that the most critical time period in which to establish the whereabouts of suspects and persons of interest was the approximately six hours surrounding the time of the murder." RA 31.

meaning of *Augustine*, this Court should reaffirm that where, as here, the Commonwealth warrantlessly obtains two weeks of CSLI, no portion of that location information has been lawfully obtained.

II. A Temporal Exception to the Warrant Requirement for CSLI Is Not Necessary to Protect the Public.

As discussed above, *Augustine* squarely controls this case. Nevertheless, the Superior Court's flawed reasoning provides an opportunity to emphasize that a temporal exception is unnecessary as a doctrinal matter. Even if the Court requires a warrant for all cases in which police seek to obtain CSLI, long-recognized exceptions to the warrant requirement — such as exigent circumstances — would allow the Commonwealth to access limited amounts of CSLI without a warrant under the appropriate circumstances. Relying on such traditional exceptions, courts and legislatures throughout the country have established a bright-line rule requiring law enforcement to obtain a warrant for CSLI regardless of the length of time at issue.

A. Traditional Warrant Exceptions Make a Specific Temporal Exception to the Warrant Requirement for CSLI Unnecessary to Protect the Public.

"It is a cardinal principle that searches conducted outside the judicial process, without prior

approval by judge or magistrate, are per se unreasonable under both the Fourth Amendment to the United States Constitution and art. 14 — subject only to a few specifically established and well-delineated exceptions." *Commonwealth* v. *Bostock*, 450 Mass. 616, 623-24 (2008) (quotations and citations omitted); see also *Katz* v. *United States*, 389 U.S. 347, 357 (1967). These exceptions provide the rubric by which courts evaluate warrantless searches, and they are justified by concerns such as exigent circumstances created by a threat to officer safety or the possibility of destruction of evidence. *Warden, Md. Penitentiary* v. *Hayden*, 387 U.S. 294, 298-99 (1967).

There may be some instances, such as a missing persons case, in which the police must quickly obtain a brief period of location information. However, a bright-line rule subjecting all CSLI requests by the Commonwealth to the traditional warrant requirement would not unduly hamper such investigations, because "they are better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances." *Riley* v. *California*, 134 S. Ct. 2473, 2486 (2014).

In fact, the U.S. Supreme Court recently confronted a similar argument in *Riley*, in the context of deciding whether to permit law enforcement to

search the data on a cell phone pursuant to the search incident to arrest exception to the warrant requirement. The government claimed that concerns over loss of evidence on a phone meant police needed the ability to search the phone incident to arrest. *Id.* at 2486. The Supreme Court rejected that argument, noting that officers could rely on the "exigent circumstances" exception when supported "in each particular case" rather than the blanket search incident to arrest exception. *Id.* at 2487.

The same approach easily applies here. Where an exigency requires police to obtain CSLI immediately, they will be able to do so without a warrant in proper circumstances. Under a bright-line rule, the Commonwealth would not be precluded from introducing the fruits of a warrantless search in a court proceeding as long as it could justify the search with exigent circumstances or any other recognized warrant exception.

B. The Adoption of Bright-line Warrant Requirements for CSLI by Other States Confirms that the Traditional Warrant Exceptions Sufficiently Protect Public Safety.

Other states' adoptions of bright-line warrant requirements for CSLI reflect a growing nationwide

consensus that the traditional warrant exceptions are sufficient to protect public safety.

For example, *State* v. *Earls*, 70 A.3d 630 (N.J. 2013), held that cell phone users should be "entitled to expect confidentiality in the ever-increasing level of detail that cell phones can reveal about their lives." *Id.* at 644. Just as in *Augustine*, the *Earls* court noted that "no one buys a cell phone to share detailed information about their whereabouts with the police." *Id.* at 643. The New Jersey Supreme Court went on to adopt a categorical warrant requirement to protect individuals' reasonable expectation of privacy in their CSLI.

Significantly, *Earls* recognized that courts are "not able to draw a fine line across that spectrum [of technological advances] and calculate a person's legitimate expectation of privacy with mathematical certainty." *Id.* at 643. Equally notably, *Earls* considered the impact of its ruling on law enforcement and stated: "both the public and the police will be better served by a clear set of rules." *Id.* at 644. It determined that a categorical warrant requirement — combined with the well-established warrant exceptions — appropriately balanced the needs of law enforcement (including their need for clear guidance) and the privacy interests of cellphone users. *Id.*

Last year the Florida Supreme Court in *Tracey* v. *State*, 152 So.3d 504 (Fla. 2014), found that real time CSLI was also protected by a warrant requirement. Critically, it found that hinging the determination of whether constitutional privacy protections were violated "on the length of the time the cell phone was monitored was not a workable analysis" and invited the "danger of arbitrary and inequitable enforcement." *Id.* at 520-21. It therefore adopted a bright-line rule requiring the police to obtain a warrant in every instance, thus avoiding "'ad hoc, case-by-case'" determinations by individual officers. *Id.* at 521 (quoting *Riley*, 134 S.Ct. at 2491-92).

Similarly, the intermediate court in Pennsylvania has held that individuals' reasonable expectations of privacy in their real-time CSLI are protected under its state constitution by a warrant requirement. *Commonwealth* v. *Rushing,* 71 A.3d 939, 962-64 (Pa. Super. 2013), *rev'd on other grounds,* 99 A.3d 416 (Pa. 2014). In so doing, it too did not countenance the possibility of a temporal exception to the warrant requirement. *Id.* at 963-64.

The same approach has prevailed when it comes to the use of a GPS device to track a car's location. The state high courts of New York, Washington, and Oregon

have also ruled against warrantless tracking in holding that their state constitutions protect individuals' expectation of privacy in their location.[4] As with the case law involving cell phone location information in Florida, New Jersey and Pennsylvania, these courts did not adjust their reasonable expectation of privacy analyses based on the duration of time for which law enforcement obtained information, or cabin their rulings with a period of time for which a warrant would not be required.

Additionally, twelve states have dealt with this issue legislatively and have taken a bright-line approach. Seven states have passed laws that specifically require search warrants to obtain CSLI, without a temporal exception for short periods of time,[5] and similar legislation is pending before

---

[4] *People* v. *Weaver*, 909 N.E.2d 1195 (N.Y. 2009) (holding that law enforcement must obtain a warrant before using GPS technology to track a person's movements); *State* v. *Jackson*, 76 P.3d 217 (Wash. 2003) (same); *State* v. *Campbell*, 759 P.2d 1040 (Or. 1988) (holding that law enforcement must obtain a warrant before using a radio transmitter to locate a person's automobile); see also *Commonwealth* v. *Rousseau*, 465 Mass. 372 (2013) (holding that passenger had standing to challenge warrantless GPS tracking of car).

[5] See 725 Ill. Comp. Stat. Ann. 168/10; Ind. Code Ann. § 35-33-5-12; Maine Rev. Stat. tit. 16, § 648; Minn. Stat. Ann. § 626A.42(2); Mont. Code Ann. § 46-5-

Congress and in several state legislatures.[6] Five other states have enacted statutes requiring a search warrant to obtain location information generally, again without any temporal exception.[7]

III. This Court Should Reconsider *Augustine*'s Suggestion That There Is a Temporal Exception to the Warrant Requirement for CSLI.

In *Augustine*, this Court expressed reticence to set a bright-line warrant requirement for CSLI in view of the continuing evolution of cellphone technology. *Augustine,* 467 Mass. at 255 n.37. Although only a short time has passed since the *Augustine* decision, there are compelling reasons for the Court to revisit its suggestion of a temporal exception and instead institute a warrant requirement for all CSLI requests. First, *Augustine's* hypothesis that limited amounts of

---

110(1)(a); Utah Code Ann. § 77-23c-102(1)(a); Wis. Stat. Ann. § 968.373(2).

[6] See Online Communications and Geolocation Protection Act, H.R. 656, 114th Cong. (2015); S. 178, 2015-2016 Reg. Sess. (Cal. 2015); H.R. 876, 2015 Gen. Assemb., Reg. Sess. (N.C. 2015); S. 640, 78th Legis. Assemb., Reg. Sess. (Or. 2015); H.R. 2263, 84th Leg., Reg. Sess. (Tex. 2015).

[7] See Haw. Rev. Stat. § 803-44.7(b) (installation and use of a mobile tracking device); Okla. Stat. Ann. tit. 13, § 176.6(A) (same); Or. Rev. Stat. Ann. § 133.619(6) (same); 18 Pa. Cons. Stat. Ann. § 5761(c)(4) (same); S.C. Code Ann. § 17-30-140(b)(2) (same).

CSLI might not implicate individuals' reasonable expectations of privacy because it reveals little information about them is no longer applicable. As will be further explained below, even a limited duration of CSLI can now be highly revealing. Second, it is simply not possible for this Court, or lower courts tasked with interpreting this Court's rulings, to draw an objective and durable "temporal line of demarcation between when the police may not be required to seek a search warrant for historical CSLI and when they must do so." *Id.* This Court should therefore establish a bright-line rule subjecting all CSLI requests to the traditional warrant requirement.

A. Individuals Enjoy a Reasonable Expectation of Privacy in All of Their CSLI.

In *Augustine*, this Court recognized that individuals have a reasonable expectation of privacy in CSLI because of the exceptionally private information it can convey. 467 Mass. at 251-252. Nevertheless, it hypothesized "that a request for historical CSLI . . . for a period of six hours or less would not require the police to obtain a search warrant in addition to a § 2703(d) order" because that limited amount of CSLI would not implicate such weighty privacy interests. *Id.* at 255 n.37. Yet the Court refrained from drawing "a temporal line of

demarcation between when the police may not be required to seek a search warrant for historical CSLI and when they must do so" because *Augustine* was not "an appropriate case" "[b]oth because the time period for which the CSLI records were sought here was so long and because the CSLI request dates from 2004 — a virtual light year away in terms of cellular telephone technological development." *Id.*

In the decade since the facts giving rise to *Augustine* took place, cellular telephone technology has moved forward — and continues to move forward — at such a pace that any "temporal line of demarcation" this Court might draw will quickly be rendered unreasonable. *Id.* This counsels in favor of adopting a bright-line warrant requirement for CSLI, instead of temporal lines that will have to be redrawn every time technology — and its uses — further evolve. *Id.*

Moreover, today's smartphones generate a much greater volume of CSLI that is significantly more accurate and precise than the rudimentary cellphones that were in use in 2004. In his dissent in *Augustine*, then-Associate Justice Gants discussed the distinction between what he referred to as *telephone call CSLI*, where "the frequency of the location points depends on the frequency and duration of telephone calls to and from the telephone," *Id.* at 259 (Gants J.,

dissenting), and *registration CSLI*, which he described as being "for all practical purposes, . . . continuous, and therefore is comparable to monitoring the past whereabouts of the telephone user through a global positioning system (GPS)." Id. Today, this distinction is one without a difference, as the surge in mobile data use and the rise of SMS text messaging mean that today's smartphones are generating what one might instead call *transactional* CSLI on an almost-continuous basis.[8]

In *Augustine*, this Court recognized that unlike GPS tracking, which takes place on public roads, CSLI is "especially problematic, because cellular telephones give off signals from within both [public and private] spaces, and when the government seeks to obtain CSLI from a cellular service provider, it has no way of knowing in advance whether the CSLI will have originated from a private or public location."

---

[8] "Transactional CSLI" can be defined to encompass the traditional telephone call CSLI to which then-Justice Gants referred in his dissent in *Augustine*, but also to the CSLI that is generated whenever a smartphone user sends or receives information via a cellular internet connection or exchanges SMS text messages with a correspondent. Cohen, What Your Cell Phone Could Be Telling the Government, Time (Sept. 15, 2010), http://content.time.com/time/nation/article/0,8599,2019239,00.html.

Id. at 253. The tremendous accuracy of today's CSLI technology exacerbates this problem. No longer does CSLI "provide[] the approximate physical location . . . of a cellular telephone[.]" *Id.* at 259 (Gants J., dissenting). On the contrary, today's CSLI technology is often accurate to within 2 meters, or 6 1/2 feet. Pell & Soghoian, Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy, 28 Harv. J.L. & Tech. 1, 11 n.44 (2014). Such accuracy enables the Commonwealth to use transactional CSLI records from smartphones to determine whether a couple sleeps in the same room,[9] whether a drug store patron is shopping for candy or contraceptives, or whether someone in a courtroom is a member of the bench, the bar, or the public. As the Supreme Court of the United States observed in *Riley*, "[h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the

[9] According to a recent study by the Pew Reserch Center, "[f]ully two-thirds (65%) of adults say they have slept with their cell phone on or right next to their bed." Lenhart, Cell Phones and American Adults, Pew Research Center, at http://www.pewinternet.org/2010/09/02/cell-phones-and-american-adults/ (last viewed Apr. 22, 2015).

minute, not only around town but also within a particular building." 134 S. Ct. at 2490.

The striking nature of this increased detail can be seen in an example from Germany. In 2011, a politician named Malte Spitz successfully sued Deutsche Telekom, which operates the T-Mobile cellular telephone network in Germany, the United States, and eleven other countries, to obtain 180 days of transactional CSLI generated by his smartphone that the company had collected. See Tell-All Telephone, Die Zeit — Zeit Online, at http://www.zeit.de/datenschutz/malte-spitz-data-retention (last viewed April 22, 2015). During this period, Deutsche Telekom amassed 35,830 transactional CSLI records generated by Mr. Spitz's voice conversations, Internet usage, and SMS text message communications on his smartphone.[10] On

[10] The raw historical CSLI data that Mr. Spitz obtained from Deutsche Telekom is available as a spreadsheet at http://www.zeit.de/datenschutz/malte-spitz-data-retention (press the "download data" button located at the lower right hand corner of the screen) (last accessed April 22, 2015). Columns A and B of the spreadsheet, entitled "Beginn" and "Ende" respectively, provide the date and time that each of Mr. Spitz's cellular telephone transactions began and ended. Column C identifies whether these transactions were voice conversations, SMS text messages, or internet data transmissions using the terms "telefonie," "SMS," and "GPRS," respectively. Column D, entitled "ein/ausgehend," identifies whether the transmissions were outgoing ("ausgehend") or incoming

average, therefore, Deutsche Telekom collected 8.3 transactional CSLI records per hour from Mr. Spitz's smartphone, or one locational record every seven minutes and 14 seconds.

As Mr. Spitz's records indicate, however, not all time periods generate equal quantities of transactional CSLI records. In the middle of the night, when Mr. Spitz was presumably asleep, his smartphone generated just two transactional CSLI records per hour. When he was stationary, a transactional CSLI record was generated every time he made or received a phone call, sent or received an SMS text message, or whenever his smartphone accessed data on the Internet — either through Mr. Spitz's active use of his smartphone, or by the automatic data refresh features that are common to most smartphone platforms and applications. See, e.g., Apple, Understand Multitasking and Background Activity on Your iPhone, iPad, or iPod Touch, available at https://support.apple.com/en-us/HT202070 (last accessed April 22, 2015). More significantly, however, when Mr. Spitz was in motion, transactional CSLI

("eingehend"). Columns E and F, entitled "Laenge" and "Breite," record Mr. Spitz's longitude and latitude, respectively, at the time of each transaction.

records were generated by his phone on a minute-by-minute basis, as his calls were handed off from one cellular transmitter to another.

Thus, while the dissent in *Augustine* may have correctly described the technology relevant at the time as "provid[ing] the approximate physical location (location points) of a cellular telephone only when a telephone call is made or received by that telephone," *Augustine*, 467 Mass. at 259 (Gants J., dissenting), this is no longer true. The transactional CSLI generated by smartphones provides a near-continuous record of a subscriber's location, simply by virtue of the device being switched on.

Finally, even small amounts of transactional and registration CSLI now implicate the reasonable privacy interests of individuals not only because they paint a detailed picture of where we were, but also because this information can be used to predict where we will be with astonishing accuracy.

In 2010, researchers at Harvard and Northeastern Universities found that cell phone location records can predict where a person *will be* at any given time with 93-percent accuracy. Song et al., Limits of Predictability in Human Mobility, 327 Science 1018 (2010). Similarly, in 2013, an MIT-led research team was able to take a database containing anonymized CSLI

records for 1.5 million people, and then re-identify individuals with 95% accuracy based on just four locational records per person. de Montjoye et al., Unique in the Crowd: The Privacy Bounds of Human Mobility, 3 Scientific Reports 1376 (2013), at http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html.

As the volume and accuracy of CSLI continues to grow, and as our electronic devices collect more and more data about us, the correlation of these various data streams with CSLI can paint an ever more accurate picture of not only "a person's public movements that reflect[] a wealth of detail about her familial, political, professional, religious, and sexual associations", *Jones*, 132 S. Ct. 945, 955 (Sotomayor J., concurring), but also reflect our private movements and intimate associations as well. See also *Tracey*, 152 So. 3d at 523 (cell phone tracking "can reveal a detailed and intimate picture of the user's life"); *Earls*, 214 N.J. at 586 ("details about the location of a cell phone can provide an intimate picture of one's daily life.").

In this new context, "the duration of the period for which historical CSLI is sought" can no longer be "a relevant consideration in the reasonable expectation of privacy calculus . . . ." *Augustine*,

467 Mass. at 254. There is no longer "some period of time for which the Commonwealth may obtain a person's historical CSLI by meeting the standard for a § 2703(d) order alone, because the duration is too brief to implicate the person's reasonable privacy interest." *Id.* Unlike GPS vehicle location tracking, which "impacts a privacy interest on the part of the individual who is the target of the tracking" "only when such tracking takes over extended periods of time," *id.* at 253, our cellphones track us every minute of every day – regardless of where we go – and generate records of our past movements that allow law enforcement to track us back in time. *Id.* at 252-253. The only way to protect individuals' privacy interest in this highly revealing information is with a bright-line warrant requirement.

B. The Temporal Exception to the Warrant Requirement Has Proven Unworkable in Practice

In addition to underprotecting privacy interests, *Augustine's* suggested temporal exception has proven unworkable in practice. Lower court judges are experiencing great difficulty in applying the temporal exception articulated in *Augustine*, and what is now emerging is precisely the sort of patchwork of decisions where judges and law enforcement are forced to make ad hoc determinations of the kind that courts

strive to avoid. See, e.g., *Oliver* v. *United States*, 466 U.S. 170, 181 (1984) ("Nor would a case-by-case approach provide a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment.").

In addition to this case — where the lower court found the collection of two weeks of CSLI without a warrant did not violate Article 14 or *Augustine* — there have been at least three other cases decided in the 15 months since *Augustine* was issued that point to confusion in the absence of a bright-line rule.

In *Commonwealth* v. *Princiotta,* No. 2009-0965, 2014 WL 5317765 (Mass. Super. Oct. 9, 2014), the Bristol Superior Court denied the defendant's motion to suppress 29 hours of CSLI obtained without a warrant, holding that "law enforcement's collection of twenty-nine hours of . . . CSLI records failed to implicate the defendant's privacy interest." *Id.* at *4. The court noted that "*Augustine* does not establish a categorical rule barring use of the reasonable suspicion standard in authorizing production of historical CSLI pursuant to a § 2703(d) order." *Id.* at *2. Even though the 29 hours of CSLI was nearly five times longer than the six-hour period contemplated by *Augustine*, the court nevertheless found this was "too small of a sample size for the police to make any

conclusions about the defendant's habits or personal routine." *Id.* at *3. It emphasized that the "brief period" of CSLI "was *intended* to identify the defendant's location before, during and after the shooting, and to locate evidence that may have been hidden or partially destroyed after the commission of a crime" rather than to "reconstruct his way of life." *Id.* at *4 (emphasis added).

In *Commonwealth* v. *Polanco*, No. BRCR2010-01465, 2014 WL 7499052 (Mass. Super. May 1, 2014), the Bristol Superior Court denied a motion to suppress nearly four days of CSLI obtained with an 18 U.S.C. § 2703(d) order rather than a warrant, finding the defendants' reasonable expectation of privacy was not violated because the order was "narrowly circumscribed around the commission of the crime and the period immediately before it." *Id.* at *1. The court provided no justification for why four days of historical CSLI could be lawfully obtained without a warrant notwithstanding *Augustine,* instead finding that the "time-limited intrusion into the defendants' privacy" was reasonable. *Id.* at *3.

In *Commonwealth* v. *Streety*, No. CRIM.A. 2013-1261, 2014 WL 3375673 (Mass. Super. Apr. 23, 2014), the Middlesex Superior Court denied a motion to suppress fourteen hours of registration CSLI that was

obtained without any judicial authorization and used to aid in the execution of an arrest warrant, despite the court's conclusion that there was a "constitutionally significant intrusion on the . . . reasonable expectation of privacy." *Id.* at *10. The court focused on the purposes for which the registration CSLI was used, expressing doubt that *Augustine*, which it believed had considered the use of CSLI for "purely investigative purposes," *id.* at *11, "would be extended to the use of CSLI to facilitate the execution of an arrest warrant." *Id.* at *13. It found that the CSLI was properly obtained because an arrest warrant diminished a person's privacy interests, consequently permitting law enforcement to obtain CSLI without a warrant.

All these cases, including the present one before this Court, highlight how *Augustine*'s six-hour window has expanded with little justification to permit acquisition of CSLI for significantly longer periods of time beyond that contemplated in *Augustine*. That is the biggest disadvantage of failing to create a bright-line rule: police and courts will be forced to make ad hoc, case-by-case decisions about when (if ever) they must get a warrant to obtain CSLI. That disadvantages not only police, who must make snap decisions and hope they are right at the risk of

having evidence excluded, but also the members of the public, who are uncertain as to when their location privacy can be intruded upon without a warrant.[11] As the Supreme Court has explained, "the protections intended by the Framers could all too easily disappear in the consideration and balancing of the multifarious circumstances presented by different cases, especially when that balancing may be done in the first instance by police officers engaged in the 'often competitive enterprise of ferreting out crime.'" *Dunaway* v. *New York*, 442 U.S. 200, 213 (1979) (quoting *Johnson* v. *United States*, 333 U.S. 10, 14 (1948)).

This Court should therefore adopt a bright-line and require police to obtain a warrant before it obtains any CSLI, regardless of the length of time sought by law enforcement.

CONCLUSION

For the reasons stated above, amici respectfully urge this Court to hold that where the Commonwealth warrantlessly obtains two weeks of CSLI, no portion of that location information is lawfully obtained, and to

[11] It of course also disadvantages cell phone providers, who will have to guess at which situations permit Massachusetts law enforcement to obtain CSLI without a warrant.

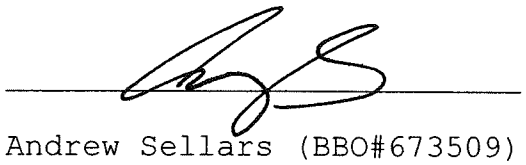
further establish a bright-line warrant requirement for all CSLI requests.

Respectfully submitted,

American Civil Liberties Union Foundation of Massachusetts

Electronic Frontier Foundation

BY THEIR COUNSEL[12]



Andrew Sellars (BBO#673509)
asellars@cyber.law.harvard.edu
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

Dated: April 24, 2015

[12] Amici thank Harvard Law School Cyberlaw Clinic students Abigail Colella, Sandra Hanian, and William Travis West for their valuable contributions to this brief.

CERTIFICATE OF COMPLIANCE

I, Andrew Sellars, 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), 17, 18, and 20.

Dated: April 24, 2015

ADDENDUM

Constitution of the United States of America
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.

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, Andrew Sellars, hereby certify that on April 24, 2015, 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:

Counsel for Jason Estabrook:

George E. Murphy, Jr.
149 Cambridge St.
East Cambridge, MA 02141

Counsel for Adam Bradley:

Daniel Beck
Law Office of Daniel Beck
52 Western Ave.
Cambridge, MA 02149

Susan M. Costa
Law Offices of Susan M. Costa
185 Devonshire St., Suite 302
Boston, MA 02210

Counsel for the Commonwealth:

Jamie Michael Charles
David Marc Solet
Michael Albert Kaneb
Assistant District Attorneys
Office of the Middlesex District Attorney
15 Commonwealth Ave.
Woburn, MA 01801

Dated: April 24, 2015