

CORRECTED

COMMONWEALTH OF MASSACHUSETTS

SUPREME JUDICIAL COURT

SUFFOLK COUNTY

NO. SJC-11482

COMMONWEALTH,
Appellant,

V.

SHABAZZ AUGUSTINE,
Defendant - Appellee.

BRIEF AND ADDENDUM
FOR DEFENDANT SHABAZZ AUGUSTINE
FROM A JUDGMENT OF THE SUFFOLK SUPERIOR COURT

Nathan Freed Wessler
BBO #680281
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

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

September 18, 2013.

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iii
ISSUES PRESENTED	1
PRELIMINARY STATEMENT	1
STATEMENT OF THE CASE	4
STATEMENT OF FACTS	4
SUMMARY OF ARGUMENT	13
ARGUMENT	17
I. The Commonwealth's acquisition of cell site location information was an unconstitutional warrantless search	17
A. The acquisition of CSLI is a search because it can precisely target a cell phone user's movements.	18
1. Extended government surveillance of a person's movements is a search.	20
2. The Commonwealth's acquisition of CSLI is a search because CSLI can be used to target an individual's movements	22
3. Augustine was not required to prove the locations revealed by the CSLI	25
B. The acquisition of CSLI is also a search because it can intrude on constitutionally-protected spaces	29
C. A cell phone provider's collection of CSLI does not eliminate the customer's reasonable expectation of privacy in that data	31

1.	The third party doctrine, particularly under article 14, applies only to voluntarily- conveyed information.	32
2.	Augustine did not relinquish any privacy interest in his cell phone's location.	35
3.	This Court should narrow its third party doctrine.	39
II.	The Superior Court did not commit reversible error by taking judicial notice of facts about CSLI	41
A.	The Superior Court correctly noticed facts that had been conceded by the Commonwealth	42
B.	Any error was harmless	45
III.	The Superior Court correctly applied the exclusionary rule	46
	CONCLUSION	50
	CERTIFICATE OF COMPLIANCE	51
	ADDENDUM	52
	RECORD APPENDIX	separately bound

TABLE OF AUTHORITIES

Cases

<u>Arizona v. Gant</u> , 556 U.S. 332 (2009)	18
<u>Commonwealth v. Antobenedetto</u> , 366 Mass. 51 (1974)	28
<u>Commonwealth v. Balicki</u> , 436 Mass. 1 (2002)	19
<u>Commonwealth v. Blood</u> , 400 Mass. 61 (1987)	<u>passim</u>
<u>Commonwealth v. Buccella</u> , 434 Mass. 473 (2001)	3, 33, 35, 36
<u>Commonwealth v. Connolly</u> , 454 Mass. 808 (2009)	2, 19, 20, 24, 47
<u>Commonwealth v. Cote</u> , 407 Mass. 827 (1990)	15, 33, 34, 35, 39
<u>Commonwealth v. DiMarzio</u> , 436 Mass. 1012 (2002)	48
<u>Commonwealth v. Feodoroff</u> , 43 Mass. App. Ct. 725 (1997)	33, 35
<u>Commonwealth v. Gomes</u> , 408 Mass. 43 (1990)	46
<u>Commonwealth v. Green</u> , 408 Mass. 48 (1990)	42
<u>Commonwealth v. Grinkley</u> , 44 Mass. App. Ct. 62 (1997)	46
<u>Commonwealth v. Hernandez</u> , 456 Mass. 528 (2010)	16, 49
<u>Commonwealth v. Jean-Charles</u> , 398 Mass. 752 (1986)	47-48
<u>Commonwealth v. Johnson</u> , 461 Mass. 44 (2011)	28

<u>Commonwealth v. King,</u> 445 Mass. 217 (2005)	41
<u>Commonwealth v. Lobo,</u> 82 Mass. App. Ct. 803 (2012)	47
<u>Commonwealth v. Montanez,</u> 410 Mass. 290 (1991)	17
<u>Commonwealth v. Moody,</u> 466 Mass. 196 (2013)	42
<u>Commonwealth v. One 1985 Ford Thunderbird Auto.,</u> 416 Mass. 603 (1993)	37
<u>Commonwealth v. Pares-Ramirez,</u> 400 Mass. 604 (1987)	48
<u>Commonwealth v. Peters,</u> 453 Mass. 818 (2009)	41
<u>Commonwealth v. Pitt,</u> 39 Mass. L. Rptr. 445, 2012 WL 927095 (Mass. Sup. Ct. 2012)	27-28, 36, 43
<u>Commonwealth v. Porter P.,</u> 456 Mass. 254 (2010)	17, 30
<u>Commonwealth v. Rousseau,</u> 465 Mass. 372 (2013)	<u>passim</u>
<u>Commonwealth v. Stoute,</u> 422 Mass. 782 (1996)	19
<u>Commonwealth v. Tapia,</u> 463 Mass. 721 (2012)	47-48
<u>Commonwealth v. Tatum,</u> 466 Mass. 45 (2013)	29
<u>Commonwealth v. Upton,</u> 394 Mass. 363 (1985)	19
<u>Commonwealth v. Valerio,</u> 449 Mass. 562 (2007)	16, 46
<u>Commonwealth v. Whynaught,</u> 377 Mass. 14 (1979)	42, 43

<u>Commonwealth v. Wyatt,</u> 30 Mass. L. Rptr. 270, 2012 WL 4815307 (Mass. Super. 2012)	8, 18, 36, 42-43
<u>Davis v. United States,</u> 131 S. Ct. 2419 (2011)	16, 48-49
<u>District Attorney for the</u> <u>Plymouth District v. Coffey,</u> 386 Mass. 218 (1982)	17-18
<u>In re Application of the U.S. for</u> <u>Historical Cell Site Data,</u> --- F.3d ----, 2013 WL 3914484 (5th Cir. July 30, 2013), vacating 747 F. Supp. 2d 827 (S.D. Tex. 2010),	2, 9, 10, 43, 44
<u>In re Application of the U.S. for</u> <u>an Order Authorizing the Release</u> <u>of Historical Cell-Site Info.,</u> 736 F. Supp. 2d 578 (E.D.N.Y. 2010)	25
<u>In re Application of the U.S. for</u> <u>an Order Authorizing the Release</u> <u>of Historical Cell-Site Info.,</u> 809 F. Supp. 2d 113 (E.D.N.Y. 2011)	40
<u>In re Application of the U.S. for</u> <u>an Order (1) Authorizing The Use</u> <u>of A Pen Register and Trap and Trace</u> <u>Device and (2) Authorizing Release</u> <u>of Subscriber Info. and/or Cell Site Info.,</u> 396 F. Supp. 2d 294 (E.D.N.Y. 2005)	27
<u>In re Application of the U.S. for</u> <u>an Order Directing a Provider</u> <u>of Elec. Commc'ns Serv. To Disclose</u> <u>Records to the Gov't,</u> 620 F.3d 304 (3d Cir. 2010)	23, 36
<u>In re Application of the U.S. for</u> <u>Pen Register and Trap/Trace Device</u> <u>with Cell Site Location Auth.,</u> 396 F. Supp. 2d 747 (S.D. Tex. 2005)	10

<u>Jenkins v. Chief Justice of the Dist. Court Dep't,</u> 416 Mass. 221 (1993)	18
<u>Kyllo v. United States,</u> 533 U.S. 27 (2001)	<u>passim</u>
<u>People v. Weaver,</u> 12 N.Y.3d 433 (2009)	19
<u>See v. City of Seattle,</u> 387 U.S. 541 (1967)	30
<u>Smith v. Maryland,</u> 442 U.S. 735 (1979)	<u>passim</u>
<u>State v. Earls,</u> 70 A.3d 630 (N.J. 2013)	2, 24, 25, 43, 44
<u>Stoner v. California,</u> 376 U.S. 483 (1964)	30
<u>United States v. Jones,</u> 132 S. Ct. 945 (2012)	2, 21, 22, 24, 40
<u>United States v. Karo,</u> 468 U.S. 705 (1984)	29, 30, 31
<u>United States v. Miller,</u> 425 U.S. 435 (1976)	<u>passim</u>
<u>United States v. N.Y. Tel. Co.,</u> 434 U.S. 159 (1977)	33
<u>United States v. Powell,</u> --- F. Supp. 2d ---, 2013 WL 1876761 (E.D. Mich. May 3, 2013)	26, 30
<u>United States v. Rabinowitz,</u> 339 U.S. 56 (1950)	26
<u>United States v. Sparks,</u> 711 F.3d 58 (1st Cir. 2013)	49
<u>United States v. Warshak,</u> 631 F.3d 266 (6th Cir. 2010)	37

United States v. White,
401 U.S. 745 (1971) 34

Constitutional Provisions

Federal Constitution

Fourth Amendment passim

Massachusetts Declaration of Rights

Article 14 passim

Statutes

18 U.S.C. § 2703 passim

G.L. c. 231, § 119 41

Other Authorities

Commonwealth's Brief,
Commonwealth v. Carnes, No. SJC-10523,
2010 WL 1556524 (Mar. 2010) 23

Commonwealth's Memorandum in Opposition,
Commonwealth v. Collins, No. SUCR2007-10165
(Mass. Sup. Ct. Sept. 3, 2013) 23

Commonwealth's Brief,
Commonwealth v. Crouse, No. SJC-09020,
2006 WL 2592869 (Apr. 25, 2006) 23

Robert J. Cordy, Criminal Procedure
and the Massachusetts Constitution,
45 New Eng. L. Rev. 815 (2011) 18-19

CTIA-The Wireless Ass'n, "Wireless Quick Facts,"
[http://www.ctia.org/advocacy/
research/index.cfm/aid/10323](http://www.ctia.org/advocacy/research/index.cfm/aid/10323) 40, 44

Scott Shane and Colin Moynihan, Drug agents
use vast phone trove, eclipsing N.S.A.'s,
New York Times, Sept. 1, 2013 37-38

Testimony of Matt Blaze, House Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security Hearing on ECPA, Part 2: Geolocation Privacy and Surveillance (Apr. 25, 2013)	45-46
Nicole C. Wong, <u>Scans airport security staff sees would shock passengers, critics say</u> , Boston Globe, Aug. 11, 2008	38

Issues Presented

1. Does a cell phone user have a reasonable expectation of privacy in more than two weeks of historical cell site location information (CSLI) warrantlessly acquired from his cell phone provider?
2. If it is undisputed that CSLI is capable of providing precise location information, did the Superior Court clearly err by taking judicial notice that CSLI can determine a phone's location?
3. If the Commonwealth has unconstitutionally acquired CSLI without a warrant, and if it did so when no decision of this Court excused it from obtaining a warrant, should the evidence be suppressed?

Preliminary Statement

This appeal arises from the prosecution's claim that the Commonwealth's citizens have no constitutionally-protected interest in location data that is automatically generated when they make or receive cell phone calls. If that is so, then the government can warrantlessly target the movements of cell phone users--whether they are murder suspects, like defendant Shabazz Augustine, average citizens, or justices of this Court--without probable cause. That claim undermines the protections of article 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the United States Constitution.

The type of data at issue is historical cell site location information, or CSLI. Cell sites, which typically have three faces, receive signals from cell phones. Phone providers record the sites and faces that communicate with a phone over time. The denser the sites, the more precisely a phone's location can be determined. And a cell phone's location is, of course, a proxy for its user's

location. Here, in the hope of ascertaining Augustine's movements, the Commonwealth warrantlessly obtained over two weeks of CSLI from his cell phone provider.

Courts are divided on whether such conduct requires a warrant. On one side, the Supreme Court of New Jersey has recognized a protected privacy interest, under that state's constitution, in cell phone location data. State v. Earls, 70 A.3d 630 (N.J. 2013). On the other side, the Fifth Circuit has ruled that the Fourth Amendment does not protect such an interest. In re Application of the U.S. for Historical Cell Site Data, --- F.3d ----, 2013 WL 3914484 (5th Cir. July 30, 2013). In the present case, the Superior Court suppressed the CSLI.

That ruling was correct. This Court has held, and five Supreme Court justices have concluded, that extended government tracking of a person's movements violates a reasonable expectation of privacy. Commonwealth v. Rousseau, 465 Mass. 372 (2013); United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); id. at 957 (Alito, J., concurring in judgment). Location tracking violates a person's reasonable expectation that her "comings and goings will not be continuously and contemporaneously monitored except through physical surveillance." Commonwealth v. Connolly, 454 Mass. 808, 835 (2009) (Gants, J., concurring). Moreover, CSLI can reveal not only where people are, but where they have

been. Accordingly, the government's acquisition of CSLI should require a warrant.

The Commonwealth's contrary claim rests largely on two flawed arguments. First, it argues that CSLI is not as likely as global positioning system (GPS) data to reveal a precise location. On that basis, it argues that the court below improperly took judicial notice that CSLI "can determine a cell phone's location." SRA 263.^{1/} But CSLI's precision in a particular case is beside the point. The Commonwealth has conceded that CSLI can reveal precise locations. Comm. Br. 22, 23. And CSLI from a phone, which can be carried anywhere, is more intrusive than GPS data from a car that travels on public streets. The court below properly concluded that these undisputed capabilities trigger article 14 protection.

Second, invoking the "third party doctrine," the Commonwealth argues that a cell phone user cannot have a protected privacy interest in CSLI because it is recorded by the cell phone provider. But, under the Fourth Amendment, the doctrine applies only to information "voluntarily conveyed" to third parties. Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976). Under article 14, the doctrine is even narrower. Commonwealth v. Buccella, 434 Mass. 473, 484 n.9 (2001). This Court has recognized that, even when someone has shared information with a third party, "it is

^{1/} "SRA" is Augustine's Supplemental Record Appendix.

unreasonably intrusive to impose the risk of electronic surveillance on every act of speaking aloud to another person." Commonwealth v. Blood, 400 Mass. 61, 74 (1987). Because cell phone users do not voluntarily convey their locations when making or receiving calls, the doctrine does not apply here.

This Court should therefore affirm the ruling below and confirm that the mere "act of speaking" on a cell phone does not risk warrantless government tracking.

Statement of the Case

On July 29, 2011, the Suffolk County grand jury indicted Augustine for the murder of Julaine Jules. SRA 17. On November 15, 2012, Augustine moved to suppress evidence, including location evidence, obtained by the Commonwealth under 18 U.S.C. § 2703(d). The Superior Court (Sanders, J.), heard the motion on January 16 and February 15, 2013, and allowed it on February 26, 2013. SRA 6, 72-179, 196-235. On March 4, 2013, the Commonwealth applied for interlocutory review. SRA 240-261. Justice Sanders then issued, on April 3, 2013, a memorandum of decision. SRA 262-274. On May 2, 2013, Justice Gants allowed the Commonwealth's application and ordered that the appeal be heard by the full bench of this Court. SRA 296.

Statement of Facts

I. The CSLI Order

The Commonwealth obtained historical cell site location information about Augustine while investigating

the death of Julaine Jules. Jules disappeared on August 24, 2004, and her body was discovered in the Charles River on September 19, 2004. SRA 262. Initially her death was investigated by the Middlesex County District Attorney's Office, which used the Stored Communication Act (SCA) to seek records about Augustine's phone.

The SCA permits the government to "require" a cell phone provider "to disclose a record or other information" relating to a customer only under certain circumstances. 18 U.S.C. § 2703(c)(1). One circumstance arises when the government "obtains a warrant." Id. § 2703(c)(1)(A). Another arises when the government obtains an order under § 2703(d). Id. § 2703(c)(1)(B). Such an order requires the government to present "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." Id. § 2703(d). But an order sought by state officials "shall not issue if prohibited by the law of [the] State." Id.

On September 22, 2004, the Middlesex District Attorney's Office applied for and obtained the § 2703(d) order at issue here. SRA 15-16, 151-152. The application was accompanied by an affidavit signed by Trooper Mary McCauley. Her affidavit asserted that Augustine had been a boyfriend to Jules and had arranged to meet her on August 24, 2004--the day she disappeared--after learning that Jules had another boyfriend. McCauley stated that,

during questioning on August 28, Augustine disputed seeing Jules after August 19 and became "very upset and started to cry." SRA 11. McCauley asserted that "'tower records'" relating to Jules and Augustine could "possibly include or exclude Augustine as a suspect." SRA 14.

The Superior Court issued the § 2703(d) order to Augustine's cell provider, Sprint Spectrum. SRA 15-16. It ordered Sprint to disclose "[a]ny and all information" about "the physical location" of Augustine's phone when it made or received calls for "a 14 day period following and including August 24th, 2004." SRA 16. It also barred Sprint from disclosing the order's existence, even to Augustine. SRA 15. In support of the order, the court found "specific and articulable facts showing that there are reasonable grounds to believe that the records . . . are relevant and material to an ongoing criminal investigation." Id. There is no evidence that the Commonwealth asserted, or that the court found, probable cause.

The motion judge interpreted the order to mean that the Commonwealth was authorized to acquire CSLI for 14 days. SRA 273. But Augustine's counsel noted below, without objection, that the Commonwealth actually obtained CSLI for a longer period. SRA 207. Overall, the Commonwealth acquired roughly 100 pages of billing, call, and cell site records for Augustine's phone. SRA 24 (¶¶ 117-118).

The criminal investigation was later transferred to the Suffolk County District Attorney's Office, and Augustine was charged with murder in July 2011. SRA 17.

II. The Motion to Suppress

Augustine moved to suppress "all evidence" obtained via the § 2703(d) order, "including records that would show [his] location at a particular time." SRA 34. The motion relied primarily on the Fourth Amendment and article 14, and it was supported by affidavits from Augustine, from his friend Keisha Smith, and from his trial counsel. Augustine's affidavit asserted that he used the phone at issue, paid its bill, and never gave law enforcement "permission to access or obtain any records for that phone." SRA 36. Smith stated that she purchased the phone for Augustine's "exclusive use" and that Augustine used it and paid its bill. SRA 35. Augustine's counsel expressed a belief that the Commonwealth would use CSLI records "to pinpoint [Augustine's] travel and locations in August and September of 2004." SRA 37, 71.

The Superior Court held hearings on January 16, 2013, and February 15, 2013. At those hearings, neither party introduced into evidence the CSLI records that the Commonwealth had obtained. Nor did either party purport to show what those CSLI records, together with information about the location of Sprint's cell sites, could reveal about Augustine's movements. In fact, the Commonwealth did

not disclose the location of Sprint's cell sites until after the February hearing. SRA 236.

But the parties stipulated to two types of facts: (1) the Commonwealth's intentions with respect to the CSLI records and (2) the capabilities of CSLI technology. The parties agreed that the Commonwealth intended to use the CSLI to "gather [Augustine's] location at various times." SRA 145-146. They also agreed on how CSLI is used to determine a cell phone user's location. Augustine's counsel cited an opinion in which Superior Court Justice David Lowy took judicial notice of "how the location [of a cell phone] is determined," and asked that Justice Sanders "do this also." SRA 144, citing Commonwealth v. Wyatt, 30 Mass. L. Rptr. 270, 2012 WL 4815307 (Mass. Sup. Ct. 2012). The Commonwealth did not object. SRA 144-145.

Instead, the Commonwealth conceded the point. Its written submission stated that a cell phone communicates with a cell tower when it makes or receives a call. SRA 181. Each tower, it noted, "has three surfaces, or 'faces,' that function as antennae." Id. The Commonwealth wrote that "[m]ost cell service providers maintain [business] records . . . that identify--for any given cell phone number--the general location of the phone at a given time by the specific tower that transmitted the call and the specific 'face' of the tower that served as the antenna." Id.

The Commonwealth also agreed that CSLI "can be" as discerning as GPS data. SRA 218, 220. The prosecutor mentioned that federal Magistrate Judge Stephen Smith had "seemed to suggest that CSLI is every bit as discerning as GPS." SRA 218. The prosecutor stated that Judge Smith's account was "partially accurate which is to say that CSLI can be." Id. But the prosecutor argued that CSLI is not that precise "in every instance," because it is "limited to where those cell towers are." Id.; see In re Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010) (Smith, M.J.), vacated, 2013 WL 3914484.

Relying on its claim that CSLI is not necessarily as precise as GPS data, the Commonwealth argued that the defense had "to show in this particular case . . . that there was CSLI that was capable of producing private information." SRA 220. The defense argued that such a showing was not required because, when the Commonwealth requests CSLI, it does not know what level of detail it will reveal, such as "whether somebody is inside the house or outside the house." SRA 224.

Finally, the Commonwealth declined to argue that the §2703(d) order was supported by probable cause. Initially, the Commonwealth had suggested that if the affidavit in support of the § 2703(d) order had "made out probable cause," then "the Commonwealth might have inevitably discovered" the CSLI. SRA 152, 194-195. But, after

subsequent research and a review of Trooper McCauley's affidavit, the prosecutor stated at the February 2013 hearing that he was "not making [this] inevitable discovery argument." SRA 199. Because the Commonwealth did not argue probable cause, the defense did not contest it. SRA 210.

III. The Motion Judge's Decision

The Superior Court allowed the suppression motion on the ground that the Commonwealth's acquisition of CSLI was a warrantless search, in violation of article 14. SRA 262. A written Memorandum set forth judicially-noticed facts and the court's legal analysis. SRA 262-274.

A. Judicial Notice

Justice Sanders explained that "there was no dispute as to the relevant facts," and the parties had "agreed that this Court could take 'judicial notice' of facts relating to this technology." SRA 263. For those facts, the court looked to In re Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 897, and In re Application of the U.S. for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005).

Justice Sanders first explained how cell providers collect CSLI. SRA 263. The court noted that "cellular phones use radio waves that connect the user's handset to the telephone network." Id. These radio waves, the court wrote, "are picked up by a system of 'cell sites,'" which

comprise "a cell tower, radio transceiver, and base station controller." Id. Justice Sanders found that radio waves are transmitted to cell sites in two ways. First, they are transmitted "any time a cell phone user makes or receives a call or text message." Id. Second, through a process called "'registration,'" they are transmitted when a cell phone "periodically identif[ies] itself to a cell tower whenever a phone is on." Id.

Service providers, the court wrote, record which cell towers receive these signals and the "precise time" the signals arrive. Id. Consistent with the Commonwealth's observation that cell sites have three surfaces--each covering 120 degrees--the court wrote that providers record the "angle at which a phone's signal arrives." Id. Thus, the court noted that CSLI--reflecting data about towers, times, and angles--"can determine a cell phone's location." Id.

The court next discussed how precisely CSLI can reveal a phone's location, and that discussion is the focus of the Commonwealth's appellate argument about judicial notice. The court noted a "trend toward more extensive archiving of [CSLI]," and that "the number of towers has . . . tripl[ed] in the last decade." Id. Because there are more towers (and less space between them), the court stated that "a cell phone user's location can be pinpointed with much more exactitude, thus diminishing the difference between CSLI and . . . GPS."

SRA 263-264. But the court did not make any findings about how precisely Augustine's location could be pinpointed using the CSLI in this case.

B. Legal Reasoning

The court ruled that the warrantless acquisition of CSLI in this case violated article 14. SRA 262. The crux of its reasoning was that location-tracking technology permits "law enforcement to access information which it would never have been able to obtain by standard police surveillance techniques." SRA 273-274.

As a threshold matter, the court predicted that this Court would view government GPS tracking as an article 14 search requiring a warrant. SRA 265-270. Thus, for Justice Sanders, the key question was whether acquiring historical CSLI is, under article 14, "somehow different than" direct GPS tracking. SRA 270.

The court gave three reasons for concluding that there is no meaningful difference. First, inferring that this Court would not limit article 14 protection to "property-based notions," the court ruled that Augustine did not need to prove a trespass against his phone. Id. Second, it stated that "CSLI is now no less accurate than GPS in pinpointing location (except perhaps in remote rural areas)." SRA 271. Third, the court ruled that the third party doctrine does not apply here because cell phone users do not affirmatively convey their locations to their providers. SRA 271-272.

Elaborating on that third point, the court noted that the third party doctrine "predate[s] the digital age" and involved cases where defendants "voluntarily convey[ed]" information. The court ruled that those cases were "inapt when one applies them to CSLI" because a cell phone user is not necessarily aware that his cell provider is making and indefinitely storing records of his location, and because "there is no overt or affirmative act by the user whereby she voluntarily exposes her location to a third party." SRA 272.

Finally, the court ruled that "the duration of the monitoring is irrelevant." SRA 273. This was "particularly true where the CSLI is historical," the court reasoned, because "it allows the government to . . . literally reconstruct a person's movements." SRA 274.

Summary of Argument

I. The acquisition of historical cell site location information in this case violated the Fourth Amendment and article 14. The Commonwealth engaged in governmental action by securing and executing a § 2703(d) order, and Augustine had a subjective privacy interest in the data acquired. That acquisition was a search, requiring a warrant, because our society accepts as reasonable a privacy interest in CSLI. Pp. 17-18.

I.A. There are three reasons why a privacy interest in CSLI is reasonable. First, this Court has held that extended GPS location tracking targeted at a person's

movements is a search. Rousseau, 465 Mass. at 382. Second, it is undisputed that the Commonwealth's acquisition of CSLI can yield intrusions as profound as the one in Rousseau. Although the Commonwealth argues that CSLI is not always as precise as GPS data, it concedes that CSLI can be that precise. Third, a defendant need not prove that CSLI revealed a precise location in a particular case, because whether a search occurred never requires proof that the government found what it was looking for. Indeed, the decision in Rousseau did not depend on what the GPS data actually revealed. Pp. 18-28.

I.B. Although the Commonwealth attempts to argue that the acquisition of CSLI is less intrusive than the GPS tracking of vehicles, Comm. Br. 50, in fact the opposite is true. Unlike cars, cell phones accompany their users almost everywhere, including their homes. Acquiring CSLI about a phone therefore intrudes on constitutionally-protected spaces and, in this way, is generally more intrusive than acquiring GPS data about a car. Pp. 29-31.

I.C. The third party doctrine does not apply here. The doctrine extinguishes a defendant's Fourth Amendment rights only if he "voluntarily conveyed" to a third party precisely the information that the government later obtained, and the doctrine extinguishes a defendant's article 14 rights only under narrower circumstances, such as when the defendant intended that his information be recorded by a third party. Smith, 442 U.S. at 742-744;

Miller, 425 U.S. at 442-443; Commonwealth v. Cote, 407 Mass. 827, 834-835 (1990). Those conditions are not met in CSLI cases. Cell phone users do not voluntarily convey information about which cell sites have communicated with their phones--indeed, they do not know that information--and they certainly do not intend for such information to be recorded. Pp. 31-41.

II. The motion judge did not take improper notice of any fact, and any error was harmless. Pp. 41-42.

II.A. The motion judge correctly noted that CSLI can determine a cell phone's location. SRA 263. Again, the Commonwealth has conceded that CSLI can be as discerning as GPS data. The motion judge also correctly noted that CSLI is becoming even more precise. The Commonwealth argues that the judge improperly used this observation to make findings about the precision of CSLI in this particular case. But, in fact, the judge made no such findings, and none were necessary. Courts do not look to the information actually found when deciding whether a search has occurred. Pp. 42-45.

II.B. Even if the motion judge strayed beyond the appropriate subjects of judicial notice--for example, by stating that CSLI is "no less accurate" than GPS--any such error was harmless. SRA 271. The crucial facts here are that the Commonwealth secured an order for more than two weeks of historical CSLI, corresponding to when Augustine's phone placed or received calls; that the CSLI

was capable of disclosing precise locations, including information about Augustine's home; and that the Commonwealth did not obtain a warrant supported by probable cause. Those facts are not in dispute, and they are dispositive. Pp. 45-46.

III. The motion judge correctly excluded the CSLI obtained by the Commonwealth. This Court's exclusionary rule looks to the nature of the underlying violation, the prejudice to the defendant, and the potential to deter police misconduct. Cf. Commonwealth v. Valerio, 449 Mass. 562, 568 (2007). Here, the warrantless collection of CSLI is a substantial constitutional violation; allowing the CSLI into evidence would be highly prejudicial; and excluding it will deter future violations. Although the Commonwealth now argues that the § 2703(d) order was supported by probable cause, it waived that argument below. The Commonwealth also argues that the CSLI should be admissible because, when it acquired the CSLI, this Court had yet to address whether a warrant was required. But even the broadest reading of the "good faith" exception to the warrant requirement would not permit officers to use the absence of precedent as grounds to dispense with seeking a warrant. Cf. Commonwealth v. Hernandez, 456 Mass. 528, 533 (2010); Davis v. United States, 131 S. Ct. 2419, 2428 (2011). Pp. 46-50.

Argument

I. **The Commonwealth's acquisition of cell site location information was an unconstitutional warrantless search.**

The Commonwealth conducted an unconstitutional search, in violation of both the Fourth Amendment and article 14, by acquiring more than two weeks of data about Augustine's movements without securing a warrant supported by probable cause. A "search" has occurred if "police conduct has intruded on a constitutionally protected reasonable expectation of privacy." Commonwealth v. Montanez, 410 Mass. 290, 301 (1991); Kyllo v. United States, 533 U.S. 27, 33 (2001). "The measure of the defendant's expectation of privacy," in turn, "is (1) whether the defendant has manifested a subjective expectation of privacy in the object of the search, and (2) whether society is willing to recognize that expectation as reasonable." Montanez, 410 Mass. at 301; Blood, 400 Mass. at 68. A warrantless search, absent exigent circumstances or consent, is unconstitutional. Commonwealth v. Porter P., 456 Mass. 254, 259 (2010).

Two of those elements--government action and a subjective expectation of privacy--cannot seriously be disputed here. Although the Commonwealth argues that there was no "governmental action" in this case, Comm. Br. 28-31, that argument is misguided. Data about Augustine was not simply "turned over to the police," as in the case cited by the Commonwealth. District Attorney for the

Plymouth Dist. v. Coffey, 386 Mass. 218, 221 (1982). Instead, the Commonwealth secured and executed an order commanding Sprint to act. SRA 9-16.^{2/} Similarly, although the Commonwealth argues that Augustine lacked a subjective privacy interest in his location, Comm. Br. 44, it is undisputed that he did not permit the police to acquire it. SRA 36.

Thus, this case boils down to the final element: whether our society is prepared to accept as reasonable a person's privacy interest in CSLI held by his cell phone provider. For the reasons stated below, it is.

- A. The acquisition of CSLI is a search because it can precisely target a cell phone user's movements.**

The Fourth Amendment is a bulwark against "police entitlement[s]," Arizona v. Gant, 556 U.S. 332, 347 (2009), and that is all the more true of article 14. Adopted in response to pre-Revolutionary writs of assistance and general warrants, article 14 was intended to thwart "unchecked control over the liberty of the people." Jenkins v. Chief Justice of the Dist. Court Dep't, 416 Mass. 221, 230 (1993); see Wyatt, 2012 WL 4815307, at *4-*6. This Court "has repeatedly concluded

^{2/} If the Commonwealth means to say that an order to a third party record holder never implicates article 14, that argument simply restates its view of the third party doctrine, which is addressed infra, at Part I.C. But it is not truly a claim of government inaction. After all, if Augustine had a privacy interest in the CSLI records here, then it is hard to imagine how the Commonwealth's acquisition of them was not "governmental action."

that Article 14's protections against unreasonable searches and seizures are broader and more restrictive of police power than those of the Fourth Amendment." Robert J. Cordy, *Criminal Procedure and the Massachusetts Constitution*, 45 *New Eng. L. Rev.* 815, 821 (2011).^{3/}

Warrantless location tracking represents a powerful threat to the "liberty of the people." Tracking can yield "a highly detailed profile, not simply of where we go, but by easy inference, of our associations--political, religious, amicable and amorous, to name only a few--and of the pattern of our professional and avocational pursuits.'" Connolly, 454 Mass. at 833-834 (Gants, J., concurring), quoting People v. Weaver, 12 N.Y.3d 433, 441-442 (2009). Because CSLI triggers the same concerns as GPS tracking, acquiring it is a search under article 14 and the Fourth Amendment. The Commonwealth's contrary argument (1) misapprehends the case law, (2) overlooks undisputed facts about CSLI, and (3) mistakenly argues that the constitutionality of acquiring CSLI should be assessed after the Commonwealth acquires it.

^{3/} See, e.g., Commonwealth v. Balicki, 436 Mass. 1, 9 (2002) (under art. 14, unlike the Fourth Amendment, the plain view exception to the warrant requirement entails a showing of inadvertence); Commonwealth v. Stoute, 422 Mass. 782, 789 (1996) (under art. 14, unlike the Fourth Amendment, the police seize someone when they pursue him with the obvious intent of requiring him or her to submit to questioning); Commonwealth v. Upton, 394 Mass. 363, 373 (1985) ("[A]rticle 14 provides more substantive protection to criminal defendants than does the Fourth Amendment in the determination of probable cause.").

1. Extended government surveillance of a person's movements is a search.

Extended government tracking violates a person's reasonable expectation of privacy. Rousseau, 465 Mass. 372. Even before this Court reached that holding in Rousseau, it held that warrantlessly installing a GPS device on a defendant's minivan was a seizure violating article 14. Connolly, 454 Mass. at 811. Although the Court did not decide whether such conduct was also a search, three justices said it was. Id. at 833 (Gants, J., concurring). Justice Gants reasoned that people can reasonably expect that their "comings and goings will not be continuously and contemporaneously monitored except through physical surveillance, which requires a far greater investment of police resources and generates far less information than GPS monitoring." Id. at 835.

Relying on Connolly, the court below predicted that this Court would regard GPS monitoring as an article 14 search. That prediction was confirmed by Rousseau.

In Rousseau, the police obtained warrants to use a GPS device to monitor a truck for 31 days. The warrants were supported by an affidavit asserting that Michael Dreslinski, who owned the truck, and John Rousseau, who was at times a passenger, used the truck to commit crimes. Both Dreslinski and Rousseau argued that the warrants were not supported by probable case. Rousseau claimed that he had been searched under article 14 even though it was not his truck. This Court agreed. It held that, under article

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." 465 Mass. at 382.

That ruling did not hinge on whether the monitoring actually disclosed details about Rousseau's life. This Court did not mention what the data revealed about Rousseau's travels. Nor did it matter that, whatever those travels were, they reflected "comings and goings in public places." Id. What mattered was that, using "extended GPS surveillance," the Commonwealth had "targeted" Rousseau's movements. Id.

That focus on the "targeting" of a person's movements matched the views of five Supreme Court justices in Jones. There, law enforcement agents installed a GPS tracking device on a car driven by the defendant. Jones, 132 S. Ct. at 948. Justice Scalia's majority opinion relied on physical trespass to hold that a search had occurred. Id. at 949. Yet five justices--in opinions by Justices Alito and Sotomayor--concluded that long-term location tracking violates a reasonable expectation of privacy. Id. at 960, 964 (Alito, J., concurring); id. at 955 (Sotomayor, J., concurring). They emphasized that GPS surveillance "can generate a comprehensive record of a person's public movements at a cost far below conventional techniques, such that it may 'evade[] the ordinary checks that constrain abusive law enforcement practices.'" Rousseau,

465 Mass. at 381, quoting Jones, 132 S. Ct. at 955-956 (Sotomayor, J.), and citing id. at 963-964 (Alito, J.).

2. The Commonwealth's acquisition of CSLI is a search because CSLI can be used to target an individual's movements.

Under the reasoning of Rousseau and the persuasive concurrences in Connolly and Jones, the Commonwealth's acquisition of CSLI for Augustine's phone was a search under the Fourth Amendment and article 14. Those decisions turned neither on the particular technology that had been used nor on the data that was actually obtained. Rather, they turned on the potential of targeted government action to disclose a person's movements. CSLI presents that same potential and thus requires the same protection.

Although the Commonwealth's brief dwells on alleged shortcomings of CSLI, its potential for tracking human beings is undisputed. Most important, the Commonwealth acknowledges that historical CSLI "can be" as precise as GPS data. SRA 218, 220. The parties also agree, and the motion judge noted, that (1) cell phones send radio signals to nearby cell sites whenever a call is made or received; and (2) carriers maintain records showing which face of which cell tower communicated with a cell phone at a given point in time. SRA 181, 263; Comm. Br. 14-15. Consequently, there is no dispute that "CSLI could in theory reveal a precise location." Comm. Br. 22 (emphasis added); Comm. Br. 23 ("[W]hether CSLI reveals a precise

location varies by customer, carrier, day.").^{4/}

Even when CSLI reveals only an imprecise location, it can still be combined with other techniques to draw precise inferences. For example, when CSLI is paired with visual surveillance or a known address, it can enable law enforcement to infer the exact location of a phone, and thus the location of its user. Cf. In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't, 620 F.3d 304, 311 (3d Cir. 2010). In fact, the Commonwealth has for years used historical CSLI in this way.^{5/} Presumably its hope in each case is to acquire data that will be precise enough to identify someone's location at a given time--or at multiple times--thus amounting to a search.

This case is no different. The Commonwealth intends to use Augustine's CSLI to "gather" his location. SRA 145-

^{4/} As discussed infra, at Part II, technological advances are enhancing the precision of CSLI. Thus, protecting a privacy interest in CSLI would be both consistent with current technology and technology that is "in development." Kyllo, 533 U.S. at 36.

^{5/} See, e.g., Comm. Br. at 22-23, Commonwealth v. Carnes, No. SJC-10523, 2010 WL 1556524 (Mar. 2010) (using CSLI from December 2005 to argue that defendant was present at the crime scene); Comm. Br. at 8-9, 16-17, Commonwealth v. Crouse, No. SJC-09020, 2006 WL 2592869 (Apr. 25, 2006) (using CSLI from July 2000 to argue that defendant visited residences to buy and sell drugs); cf. Comm. Mem. in Opp. at 23-24, 35, Commonwealth v. Collins, No. SUCR2007-10165 (Mass. Sup. Ct. Sept. 3, 2013) (contrasting call detail records (CDR) with CSLI on the ground that CDR "does not reveal, with any precision, the location of the telephone," whereas "CSLI can, in certain circumstances, reveal an individual's movements in much greater detail").

146. That intention, made possible by clear governmental action, reflects the "targeting" of Augustine's movements within the meaning of Rousseau. 465 Mass. at 382.

The monitoring was also long enough to deserve constitutional protection. For starters, the Superior Court correctly ruled that "the duration of monitoring is irrelevant." SRA 273. "[S]hort-term monitoring . . . will require particular attention" because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familiar, political, professional, religious, and sexual associations." Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring). But even if location tracking is a search only when "extended," Rousseau, 465 Mass. at 382, the tracking here meets that test. More than two weeks of CSLI is ample time to learn when a person is at home and where he goes when he is out. Cf. Connolly, 454 Mass. at 833-834 (Gants, J., concurring).

If this Court requires a warrant for such tracking, it will be in good company. The other state court of last resort to address the warrantless collection of CSLI--New Jersey's--has held that three discrete instances of CSLI collection violated a reasonable expectation of privacy protected by the New Jersey Constitution. Earls, 70 A.3d at 632. The court emphasized that "our focus belongs on the obvious: cell phones are not meant to serve as tracking devices to locate their owners wherever they may

be." Id. at 643. The court thus ruled that "[u]sers are reasonably entitled to expect confidentiality in the ever-increasing level of detail that cell phones can reveal about their lives." Id. at 644. The court also held that the state constitution "protects an individual's privacy interest in the location of his or her cell phone." Id. This Court should do the same.^{6/}

3. Augustine was not required to prove the locations revealed by the CSLI.

Despite conceding that "CSLI could in theory reveal a precise location," the Commonwealth argues that Augustine's suppression motion should have been denied because he did not prove that the records in this case "revealed any particular location." Comm. Br. 22, 43-44. That argument gets the law backward. Just as an officer's right to open someone's bag does not depend on whether the bag turns out to be empty, the constitutionality of acquiring CSLI cannot depend on what the CSLI ends up revealing.

In deciding whether government conduct amounts to a search, the relevant inquiry is not what the conduct

^{6/} The Commonwealth's acquisition of historical CSLI is no less intrusive than the real-time monitoring in Earls. See Comm. Br. 50. As the motion judge observed, historical CSLI "allows the government to do what has hitherto been impossible and literally reconstruct a person's movements in the past." SRA 274. "The picture of [a person's] life the government seeks to obtain is no less intimate simply because it has already been painted." In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 585 (E.D.N.Y. 2010).

actually revealed, but rather what it was capable of revealing. Cf. United States v. Rabinowitz, 339 U.S. 56, 80 (1950) ("The main aim of the Fourth Amendment is against invasion of the right of privacy . . . without regard to the result of such invasion."). Officers often will not know in advance what information their conduct will disclose. But that is all the more reason to regard their conduct as a search. As the Court held in Kyllo, because "[n]o police officer would be able to know in advance whether his through-the-wall surveillance picks up 'intimate' details," all such searches are "presumptively unreasonable without a warrant." 533 U.S. at 39, 40; accord United States v. Powell, --- F. Supp. 2d ----, 2013 WL 1876761, at *12 (E.D. Mich. May 3, 2013) (applying Kyllo to CSLI).

Rousseau confirms that these principles apply to location tracking. This Court's opinion did not discuss the data actually collected on Rousseau; it did not say how often or where he traveled in his friend's GPS-monitored truck. Instead, the Court emphasized that the Commonwealth had "targeted" Rousseau's movements. 465 Mass. at 382.

This Court should reach the same result here, as the Commonwealth similarly "targeted" Augustine's movements. It sought data that could be used "to determine, or assist in determining" the location of Augustine's phone when it placed or received calls--even unanswered calls--from

August 24 through September 7, 2004. SRA 16. The success of that targeting depended largely on two facts--the density of the relevant cell sites and the frequency of Augustine's calls--that the police could not know in advance. SRA 218, 220; Com. Br. 22, 23. Thus, they had no reason to assume that their conduct would safeguard Augustine's privacy. It is true that neither the actual CSLI, which was disclosed before the suppression hearings, nor Sprint's cell site locations, which were not, are in the record. But that is irrelevant; because the Commonwealth knew (and hoped) that the CSLI could produce protected information, acquiring it was a search. See In re Application of the U.S. for an Order (1) Authorizing The Use of A Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 323 (E.D.N.Y. 2005) ("Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking . . . which routinely require probable cause.").

A contrary approach would have devastating practical consequences. Most important, it could not prevent the unconstitutional acquisition of CSLI, because deterrence is impossible "if a court determines whether a warrant is required only after . . . the incursion into a citizen's private affairs has already taken place." Commonwealth v.

Pitt, 39 Mass. L. Rptr. 445, No. 2010-0061, 2012 WL 927095, *7 (Mass. Sup. Ct. 2012). It also could not remedy most constitutional violations affecting innocent people. People who are not charged with crimes generally do not learn that their CSLI has been collected. See SRA 15 (ordering Sprint not to disclose the order).

In short, because the police cannot be sure that acquiring CSLI will reveal only vague information, they cannot search first and confront the constitution later.

For the same reason, this Court should decide this case based on the facts known to the Commonwealth when it secured the § 2703(d) order: it knew what the order could reveal, but not what it would reveal.^{1/} Because the order was capable of yielding precise information, it was a warrantless search. Kyllo, 533 U.S. at 39-40. It was the Commonwealth's burden at the suppression hearing to establish some exception to the warrant requirement. Commonwealth v. Johnson, 461 Mass. 44, 48-49 (2011), citing Commonwealth v. Antobenedetto, 366 Mass. 51, 57 (1974). Yet it did not do so.^{2/} Accordingly, this Court should uphold the suppression order.

^{1/} Nevertheless, if called upon, Augustine's counsel would supplement the record with CSLI reflecting the extent of the intrusion in this case.

^{2/} Thus, even if the CSLI records somehow could have supplied evidence rendering the search constitutional after the fact--though that is impossible--it was the Commonwealth's burden to introduce such evidence "if it exist[ed]." Antobenedetto, 366 Mass. at 58.

- B. The acquisition of CSLI is also a search because it can intrude on constitutionally-protected spaces.

The Commonwealth's attempt to distinguish cases involving GPS tracking of vehicles is flawed for an additional reason: while there are practical limits on where a GPS tracking device attached to a vehicle can go, people carry their phones wherever they go, including their homes. In this way, the tracking of vehicles is less intrusive than the tracking of cell phones. Because this Court has already held that a warrant is required for the first, a warrant requirement is particularly appropriate for the second.

The "sanctity of the home is of central concern in jurisprudence concerning the Fourth Amendment to the United States Constitution and the art. 14 of the Massachusetts Declaration of Rights." Commonwealth v. Tatum, 466 Mass. 45, 56 (2013). This Court and the Supreme Court have repeatedly held that government intrusion into protected spaces, such as private homes, presumptively requires a warrant. Id.; United States v. Karo, 468 U.S. 705, 714-15 (1984). In Karo, the Supreme Court held that using an electronic device (a beeper) to draw inferences about "location[s] not open to visual surveillance," like whether "a particular article is actually located at a particular time in the private residence," was just as unreasonable as searching the location without a warrant. Id. at 714-15. Such tracking, the Court ruled, "falls

within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, id. at 707, even when it reveals that information through inference. This logic applies equally to article 14, under which "all details [in the home] are intimate details because the entire area is held safe from prying government eyes." Porter P., 456 Mass. at 260 (alteration and emphasis in original), quoting Kyllo, 533 U.S. at 37.

Under the logic of these cases, tracking cell phones is more invasive than tracking vehicles. A moving car is typically in public view. But a cell phone can reveal its owner's location at any time, even when the phone and its user are out of public view. That is because cell phones are "carried with a person wherever they go." Powell, 2013 WL 1876761, at *13 (emphasis in original). Thus, unlike cars, cell phones can be tracked into constitutionally-protected spaces. See Kyllo, 533 U.S. at 31 (homes); See v. City of Seattle, 387 U.S. 541, 543 (1967) (business premises); Stoner v. California, 376 U.S. 483, 486-88 (1964) (hotel rooms). "If at any point a tracked cell phone signaled that it was inside a private residence (or other location protected by the Fourth Amendment), the only other way for the government to have obtained that information would be by entry into the protected area, which the government could not do without a warrant." Powell, 2013 WL 1876761, at *11.

These principles confirm that Augustine's expectation of privacy in the location of his cell phone was just as reasonable, if not more reasonable, than the defendant's expectation of privacy in Rousseau. The GPS device there disclosed Rousseau's location only when he traveled in his friend's truck. Here, the Commonwealth secured an order capable of disclosing Augustine's location in any place, at any time, for over two weeks. Even assuming that Augustine's CSLI is not itself precise enough to prove at all times when he was at home--or a friend's house, or a doctor's office--it could have enabled law enforcement to infer that information. Thus, acquiring the CSLI was a search. See Kyllo, 533 U.S. 27, 36 (2001) (rejecting "the novel proposition that inference insulates a search," noting that it was "blatantly contrary" to Karo, "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home").

C. A cell phone provider's collection of CSLI does not eliminate its customer's reasonable expectation of privacy in that data.

Justice Sanders correctly ruled that, because Augustine did not voluntarily convey CSLI to Sprint, Sprint's collection of that information did not defeat Augustine's reasonable expectation of privacy in it. The Commonwealth's contrary argument misreads Fourth Amendment case law, which is distinguishable, and ignores article 14 case law, which is even less favorable to the government. Comm. Br. at 31-41. Under a correct reading

of the Fourth Amendment, and certainly under article 14, the third party doctrine does not apply here.

1. **The third party doctrine, particularly under article 14, applies only to voluntarily-conveyed information.**

Neither the federal nor state third party doctrines assist the Commonwealth. Applying the Fourth Amendment, the Supreme Court has held that defendants relinquished an otherwise reasonable expectation of privacy by voluntarily conveying to third parties precisely the information that was later obtained by the government. Smith, 442 U.S. at 742-744; Miller, 425 U.S. at 442-443. In Miller, federal agents subpoenaed an individual's bank records; in Smith, the police used a pen register to record the numbers that someone dialed from his home telephone. 425 U.S. at 437-438; 442 U.S. at 737. The Supreme Court ruled that both Miller and Smith lacked a reasonable expectation of privacy in those records, but not merely because a third party had obtained the relevant information. Instead, the Court reasoned that the records contained only information voluntarily conveyed to the third parties. Miller, 425 U.S. at 442 ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks[.]"); Smith, 442 U.S. at 744 ("[P]etitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business.").

In both cases, the Supreme Court also considered the "nature" of the documents at issue. Miller, 425 U.S. at 442. In Miller, the Court emphasized that the defendant's "checks [were] not confidential communications but negotiable instruments to be used in commercial transactions." Id. Likewise, in Smith the Court noted a "pen register's limited capabilities," 442 U.S. at 742, which did not even permit a law enforcement official to "'determine . . . whether a communication existed.'" Id. at 741, quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977).

Although the Commonwealth asserts in a footnote that the same test applies under article 14, that is not so. Comm. Br. 35 n.7. Each Massachusetts case cited by the Commonwealth "recognize[s] that analysis of an expectation of privacy following entrustment to a third party might be different under art. 14" than under the Fourth Amendment. Buccella, 434 Mass. at 484 n.9; Cote, 407 Mass. at 834-835; Commonwealth v. Feodoroff, 43 Mass. App. Ct. 725, 729-730 (1997). Thus, even if a defendant lacks Fourth Amendment protection under Miller and Smith, that fact "does not compel a similar conclusion regarding the reasonableness of the defendant's expectation of privacy under art. 14." Cote, 407 Mass. at 834.

The Blood and Cote decisions bear out this distinction. Blood involved the warrantless electronic recordings of conversations between the defendant and a

third party--an informant--who consented to surveillance. 400 Mass. at 63-65. The Supreme Court had previously ruled that warrantless surveillance with "one party consent" does not violate the Fourth Amendment. United States v. White, 401 U.S. 745 (1971). Yet this Court held that such surveillance--enabled by the defendant's choice to speak with a third party--requires a warrant under article 14. Blood, 400 Mass. at 70. Despite acknowledging that a defendant "has no constitutional right to exclude the informer's unaided testimony," the Court held that it could not authorize the extra measure of intrusion occasioned by electronic surveillance. Blood, 400 Mass. at 74, quoting White, 401 U.S. at 753.

The Court's core observation could easily have been written in this case: "We conclude that it is unreasonably intrusive to impose the risk of electronic surveillance on every act of speaking aloud to another person." Id.

Elaborating on that view, the Court held in Cote that article 14 did not protect telephone messages taken for the defendant by one third party--an answering service--in response to calls placed to an altogether different third party. Specifically, Allied Answering Service had been instructed to take messages for Cote on a telephone line belonging to another third party, the Leonard Martin Insurance Company. 407 Mass. at 829. The Court ruled that Cote lacked a protected privacy interest in the messages because he had knowingly "subjected [them] to exposure,

not only to the employees of Allied but also to anyone entitled to examine the telephone records of the Leonard Martin Insurance Co." Id. at 835. Blood did not require a different outcome, the Court explained, because "both the defendant and any callers who left a message for him at Allied intended that their words be recorded." Id.

But the Court also stated that a narrower entrustment to a third party might yield a different outcome. "It may be," the Court stated, "that under art. 14 exposure of information to another party might not compel the rejection of a claim of a reasonable expectation of privacy, particularly in light of the fact that the third party here, Allied, considered the telephone message records to be confidential." Id.^{9/}

2. Augustine did not relinquish any privacy interest in his cell phone's location.

The "exposure of information" to Sprint does not defeat Augustine's expectation of privacy. Cote, 407 Mass. at 835. Augustine did not "voluntarily convey" CSLI under Miller and Smith, and thus did not extinguish his Fourth Amendment privacy interest in that information. But even if he had, any such "entrustment" did not extinguish his privacy interests under article 14. Buccella, 434 Mass.

^{9/} See also Buccella, 434 Mass. at 484 n.9 (2001) (noting that an art. 14 analysis "might be different" than a Fourth Amendment analysis of the third party doctrine); Feodoroff, 43 Mass. App. Ct. at 729-730 (holding that there is no reasonable expectation of privacy in records of dialed calls, but noting that the issue was "a closer question under art. 14 than under the Fourth Amendment").

at 484 n.9. Three factors warrant this conclusion.

First, exposing CSLI to a cell phone provider is not like voluntarily conveying phone numbers to an operator or financial information to a teller. As several Massachusetts courts have observed, with CSLI "there is no overt or affirmative act by the user whereby she voluntarily exposes her location to a third party." SRA 272.^{10/} CSLI is not intended "to be used in commercial transactions" like a bank check, Miller, 425 U.S. at 442, and it does not have only "limited capabilities" like a pen register, Smith, 442 U.S. at 742. For example, the order here sought information that could be used to determine Augustine's precise location, even if that information was generated when his phone received calls that he did not answer. SRA 16.

Although the Commonwealth argues that Augustine knowingly exposed his location simply by turning on his phone, that argument overlooks both the record and the law. As to Augustine's knowledge, the Commonwealth relies on a 2013 policy stating that Sprint collects unspecified

^{10/} See also Pitt, 2012 WL 927095, at *3 ("A cell phone subscriber takes no overt steps to communicate his physical location to a cell phone service provider."); Wyatt, 2012 WL 4815307, at *6 ("A cellular telephone user does not take any affirmative or overt steps to communicate his or her physical location to his or her service provider."); cf. In re Application for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d at 317 ("A cell phone customer has not 'voluntarily' shared his location with a cellular provider in any meaningful way.").

"information . . . about how you use the device . . . such as . . . your location." Comm. Br. 40 n.8. There is no evidence that this policy existed, or was published, or read by Augustine, in 2004.

More fundamentally, a person's privacy rights are never extinguished by mere notice that information will be accessed by someone else. Instead, "[t]he critical point" is whether the defendant's subjective expectation of privacy "is one that society would recognize as objectively 'reasonable,' 'justifiable,' or 'legitimate.'" Commonwealth v. One 1985 Ford Thunderbird Auto., 416 Mass. 603, 607 (1993). Thus, in United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010), the Sixth Circuit concluded that email users maintained an expectation of privacy in their emails, even though the email provider's customer contract specified the provider's right to access those emails in certain circumstances.

If notice alone could extinguish a reasonable expectation of privacy, then the Commonwealth could justify any intrusion simply by running television ads notifying Massachusetts residents that they are all being tracked. Likewise, the recent revelations of widespread data collection by the federal government would have the perverse effect of insulating that collection from constitutional challenge.^{11/} That cannot be right.

^{11/} See Scott Shane and Colin Moynihan, Drug agents use
(continued...)

Second, the location information possessed by cell phone users is not identical to the information in CSLI records. A user does not know, and cannot disclose, which cell sites have communicated with her phone; that data is ascertained by the provider after its equipment receives radio signals from the phone. Thus, unlike in Miller, CSLI records do not "contain only information voluntarily conveyed to the [third party]." 425 U.S. at 442.

True, a user might know other location information--such as her phone's physical address--and she might guess that service providers ascertain phone locations in order to connect calls. But allowing a third party to glean information is, particularly under Blood, not the same thing as actively sending that information to the third party. 400 Mass. at 70-74: If ascertainment were enough, then backscatter x-rays to which people submit at the airport--which generate images of the human body^{12/}--arguably extinguish each passenger's privacy interest in what she looks like naked. That cannot be right either.

Third, particularly under article 14, cell phone users have not relinquished a privacy interest in CSLI because they have not asked that the information be

^{11/}(...continued)
vast phone trove, eclipsing N.S.A.'s, New York Times, Sept. 1, 2013, at A1.

^{12/} See, e.g., Nicole C. Wong, For their eyes only: scans airport security staff sees would shock passengers, critics say, Boston Globe, Aug. 11, 2008, at 5.

recorded. In Cote, this Court emphasized that "both the defendant and any callers who left a message for him . . . intended that their words be recorded" by the answering service. 407 Mass. at 835. The Court also distinguished Blood, where "at least one party to the conversation was unaware of the fact that their words were being recorded." Id. Here, even if Augustine had voluntarily conveyed CSLI to Sprint, or if he had knowingly permitted Sprint to ascertain his location, it would not follow that Augustine intended that Sprint record that information.

Nor is there evidence that other cell phone users, whether in 2004 or today, intend that their CSLI be recorded. Unlike telephone messages, bank statements and telephone bills, CSLI records are not provided to cell phone users, as part of their bills or otherwise. That is why the Commonwealth is constrained to rely on Augustine's mere "use of his cell phone." Comm. Br. 40. But just as "it is unreasonably intrusive to impose the risk of electronic surveillance on every act of speaking aloud to another person," Blood, 400 Mass. at 74, it is unreasonably intrusive to impose the risk of CSLI collection on every act of using a cell phone.

3. This Court should narrow its third party doctrine.

If this Court concludes that its third party doctrine applies here, then it should scale back that doctrine at least with respect to cell phone location data. The doctrine is "reminiscent of a bygone era in constitutional

jurisprudence," which does not reflect the realities of modern life. Blood, 400 Mass. at 70 n.11. "[T]he premise that an individual has no expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring).

Cell phones are perhaps the best example of these changing times. There are more than 326 million active wireless subscriptions in the United States.^{13/} "For many Americans, there is no time in the day when they are more than few feet away from their cell phones." In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011). Their phones regularly identify themselves to nearby cell sites, regardless of whether a call is made. SRA 272. It is therefore "idle to speak of 'assuming' risks in contexts where, [as here], individuals have no realistic alternative." Smith, 442 U.S. at 749-750 (Marshall, J., dissenting).

Narrowing the third party doctrine would also preserve the rule created by Rousseau. That case's limitation on warrantless tracking will have minimal

^{13/} See CTIA-The Wireless Ass'n, "Wireless Quick Facts," at <http://www.ctia.org/advocacy/research/index.cfm/aid/10323> (last visited Sept. 16, 2013).

effect if the police can warrantlessly track everyone using their own cell phones. Worse yet, the Commonwealth's position seems to imply that abundant personal information, though occasionally protected by statute, is unprotected by the Fourth Amendment or article 14. This information might include:

- the location of every child with a cell phone;
- every show a person watches on TiVo or Netflix;
- the sender and recipient of every piece of mail; and
- the comings and goings of any homeowner with a third-party-operated security system.

This Court should reject that outcome. As it has done before, the Court should revise a doctrine that has become "outmoded," "invalid," and contrary to "current knowledge." Commonwealth v. King, 445 Mass. 217, 229, 240-241 (2005) (revising the decades-old "fresh complaint" doctrine in rape cases).

II. The Superior Court did not commit reversible error by taking judicial notice of facts about CSLI.

The Superior Court's judicial notice of facts about CSLI was not error at all, let alone reversible error. This Court "accept[s] as true the subsidiary findings of fact made by the judge absent clear error[.]" Commonwealth v. Peters, 453 Mass. 818, 822-823 (2009). A harmless error not affecting substantial rights is not grounds for disturbing a lower court's judgment. G.L. c. 231, § 119. Here, given the Commonwealth's concession that CSLI can be as precise as GPS data, and given the centrality of

that fact to the core legal issue, the judge's approach was neither erroneous nor unduly prejudicial.

A. The Superior Court correctly noticed facts that had been conceded by the Commonwealth.

The Commonwealth devotes many pages to its judicial notice argument, and they all proceed from an incorrect premise. The Commonwealth asserts that the motion judge found that "the CSLI in this instance revealed . . . as precise a location as GPS." Comm. Br. 10 (emphasis added). In fact, the judge made no findings about, and took no notice of, locations in this case. And for good reason. The constitutional analysis does not turn on revelations about Augustine's location, see supra Part I, and no such revelations were possible because the Commonwealth had not disclosed Sprint's cell sites. SRA 236. Instead, the judge correctly took notice of CSLI technology in general.

A court may take judicial notice of facts that are "a subject of generalized knowledge readily ascertainable from authoritative sources." Commonwealth v. Green, 408 Mass. 48, 50 n.2 (1990). Such notice is appropriate in cases involving scientific facts. Commonwealth v. Whynaught, 377 Mass. 14, 17-18 (1979) (taking judicial notice that radar is an accurate and reliable measure of speed). Thus, this Court has looked to authoritative sources for information about cell phone technology, see Commonwealth v. Moody, 466 Mass. 196, 209 n.9 (2013) (quoting a congressional report), and many courts have taken judicial notice of facts about CSLI. See Wyatt, 2012

WL 4815307, at *1 n.5; Pitt, 2012 WL 927095, *1 n.1 ("As with radar, courts which have considered the constitutional implications of CSLI have uniformly recognized the underlying scientific principles related to how that information is obtained and used."); In re Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 831-833; cf. Earls, 70 A.3d at 636-638 (drawing on "congressional testimony" and "other sources," without expressly taking judicial notice).

These decisions confirm that, even if CSLI sometimes provides only a general location for a cell phone, it "can provide an intimate picture of one's daily life." Earls, 70 A.3d at 642. The judge below was entitled to, and did, rely on those decisions and sources to observe that "one can determine a cell phone's location" using CSLI. SRA 263; cf. Whynaught, 377 Mass. at 17-18 (relying partly on other courts' judicial notice of radar's accuracy).

The judge's observation was supported by yet another source: the Commonwealth itself. Although the Commonwealth correctly states that there was a dispute below "as to the precision that CSLI reveals a location at any given time," Comm. Br. 21, there was no dispute that CSLI "can be" as discerning as GPS data. SRA 218, 220. To this day, the Commonwealth concedes that "CSLI could in theory reveal a precise location," and whether it does so "varies by customer, carrier, and day." Comm. Br. 22, 23. Similarly, although the Commonwealth now asserts that the findings

of Judge Lowy in Massachusetts and Magistrate Judge Smith in Texas were "improper," Comm. Br. 17, below it agreed that those findings were "partially accurate[,] which is to say that CSLI can be" as accurate as GPS; it simply insisted that CSLI is not as discerning as GPS "in every instance." SRA 218.

Thus, the judge's key observation--that CSLI can determine a phone's location--is true, undisputed and dispositive. SRA 263. The judge did not rely on that observation to draw an inference about what CSLI records revealed about Augustine's movements in particular. Such an inference was entirely unnecessary.

The judge also discussed trends and changes in CSLI technology. See, e.g., SRA 263-264 (noting that the "tripling" of the number of cell towers in the last decade was "diminishing the difference" between CSLI and GPS). This forward-looking approach was appropriate; even the Commonwealth seems to understand that it is only a matter of time before CSLI becomes uniformly precise, instead of intermittently so.^{14/} The Superior Court was not required to ignore that inevitability, and neither should this Court. As the Supreme Court has cautioned in a case

^{14/} Indeed, its only complaint about the judge's account of CSLI trends is that there is "no way" to know whether the number of cell towers has tripled. Comm. Br. 24. But, in fact, there is. From 2000 to 2012, "the number of cell towers in the United States increased from 104,288 to 301,779." Earls, 70 A.3d at 637; see "Wireless Quick Facts," supra n.13; In re Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 832 & n.33.

involving a "relatively crude" thermal imaging device--far cruder, in fact, than CSLI--"the rule we adopt must take account of more sophisticated systems that are already in use or in development." Kyllo, 533 U.S. at 36.

Thus, the motion judge correctly noticed both technological trends and CSLI's capacity to reveal precise locations. The judge did not improperly notice facts about the precision of CSLI in this case because, consistent with the governing law, she took no notice of those facts.

B. Any error was harmless.

Even if the lower court had improperly noticed some fact, that error would not require reversal. The crucial judicially-noticed fact, which the Commonwealth has repeatedly conceded, is that CSLI can reveal a precise location. No other fact noticed by the Superior Court was material to the court's decision.

For example, even if Justice Sanders went too far in writing that "through a process of 'triangulation' among different towers, CSLI is now no less accurate than GPS in pinpointing location," SRA 271, this error was harmless. The judge was not making findings about the use of triangulation or other emerging technologies "in this instance." Comm. Br. 26. Nor is this fact material to the constitutional analysis.^{15/}

^{15/} It was also not far off. "Under some circumstances," CSLI technology "permits the network to calculate users' locations with a precision that approach[e] that of GPS."
(continued...)

Finally, if this Court's understanding of CSLI technology varies from the lower court's, this Court can itself take notice of pertinent facts reflected in court cases and other authoritative sources. See Commonwealth v. Grinkley, 44 Mass. App. Ct. 62, 69 n.9 (1997) ("judicial notice can be taken by trial and appellate courts"). Accordingly, if this Court concludes that there is a constitutionally-protected privacy interest in CSLI records, it should affirm the order below without remanding for additional fact-finding.

III. The Superior Court correctly applied the exclusionary rule.

The Superior Court correctly excluded the CSLI records. Massachusetts courts invoke the exclusionary rule when (1) the legal violation undermines the principles of the governing rule of law, and (2) exclusion will tend to deter future violations. Commonwealth v. Gomes, 408 Mass. 43, 46 (1990). Applying this test, courts focus on the purposes of the underlying rule, the prejudice to the defendant, and the potential to deter police misconduct. Cf. Valerio, 449 Mass. at 568. All of those factors indicate that exclusion is appropriate here.

First, freedom from government tracking is a fundamental aspect of article 14. As this Court held in

^{15/} (...continued)

Testimony of Matt Blaze at 2, House Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security Hearing on ECPA, Part 2: Geolocation Privacy and Surveillance (Apr. 25, 2013).

Rousseau, article 14 protects individuals' reasonable expectations that they will not be subjected to extended electronic surveillance by the government without a warrant supported by probable cause. 465 Mass. at 382. Targeting a person's movements through the warrantless collection of CSLI undermines the underlying principle that our comings and goings will not be continuously monitored by the government absent probable cause. See Connolly, 454 Mass. at 835 (Gants, J., concurring).

Second, the Commonwealth's violation prejudiced Augustine because the CSLI could play a significant role in the Commonwealth's prosecution, SRA 145-146, and because it is not at all certain that the government could have secured a warrant. Cf. Commonwealth v. Lobo, 82 Mass. App. Ct. 803, 808-810 (2012) (no prejudice for unlawfully ordering defendant out of the car based on the odor of marijuana where there was an independent basis to request the defendant's identification and an outstanding warrant). True, the Commonwealth now asserts that the affidavit supporting the § 2703 order supplied "probable cause" to believe that it "would furnish evidence relative to the investigation." Comm. Br. 56. But that is not the "probable cause" that matters under article 14. As the motion judge explained, SRA 274, an article 14 search must be supported by "'probable cause to believe that evidence of the crime,'" and not just evidence relative to the investigation, "'will be found in the place to be

searched.'" Commonwealth v. Tapia, 463 Mass. 721, 725 (2012) (emphasis added), quoting Commonwealth v. Jean-Charles, 398 Mass. 752, 757 (1986).

Perhaps for that reason, the Commonwealth expressly abandoned its probable cause argument--which it dubbed "inevitable discovery"--at the February 2013 hearing. SRA 152-153, 199. Thus, neither the judge who granted the order nor the motion judge were presented with or addressed the issue of probable cause. The argument has therefore been waived. Commonwealth v. DiMarzio, 436 Mass. 1012, 1013 (2002); Commonwealth v. Pares-Ramirez, 400 Mass. 604, 609 (1987).

Third, applying the exclusionary rule is necessary to deter future violations. A cell phone user whose data is collected under § 2703(d) most likely will not learn of that collection unless he is charged with a crime. Here, Sprint was ordered not to disclose the § 2703(d) order's existence. SRA 15. The only way to ensure that this information is properly collected is to exclude unlawfully collected data from criminal trials.

Finally, although the Commonwealth suggests that the exclusionary rule should not apply because this case involves an unsettled legal question, Comm. Br. 55-58, the exclusionary rule should apply for precisely that reason. The Commonwealth's approach would go far beyond the United States Supreme Court's recent holding that the federal government can avoid the exclusionary rule "when the

police conduct a search in objectively reasonable reliance on binding judicial precedent" that is later overturned. Davis, 131 S. Ct. at 2428.

To begin, Massachusetts does not recognize the "good faith" exception, "focusing instead on whether the violations are substantial and prejudicial." Hernandez, 456 Mass. at 533. But even if Davis were controlling here, it would hardly permit the police to avoid the exclusionary rule by conducting a search in reliance on the absence of binding precedent. Davis "is not a license for law enforcement to forge ahead with new investigative methods in the face of uncertainty as to their constitutionality." United States v. Sparks, 711 F.3d 58, 67 (1st Cir. 2013). Yet that is what happened here. In 2004, there was no case providing--and thus no reason to assume--that the federal Stored Communications Act satisfied the Massachusetts Declaration of Rights. What is more, the Commonwealth could have sought CSLI by applying for a warrant under § 2703(c) (1) (A). Yet it chose to use the less demanding standard of § 2703(d), without any assurance that doing so would satisfy article 14.

If the Commonwealth is permitted to skirt the exclusionary rule whenever it can point to some novel practice that is not "clearly unconstitutional on its face," Comm. Br. 56, then criminal defendants will have no incentive to challenge novel government practices in court. Those practices would then proliferate, with the


Commonwealth safe in the knowledge that any evidence obtained in violation of article 14 would either not be challenged in court or else admitted into evidence despite a successful court challenge. That result would pervert, rather than advance, the purposes of the exclusionary rule. This Court, accordingly, should reject it.

Conclusion

The Superior Court's order allowing Augustine's motion to suppress should be affirmed.

Respectfully Submitted,

Nathan Freed Wessler
BBO #680281
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org



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

September 18, 2013.