SJC-11482

COMMONWEALTH vs. SHABAZZ AUGUSTINE.

Suffolk. October 10, 2013. - February 18, 2014.

Present: Ireland, C.J., Spina, Cordy, Botsford, Gants, Duffly, & Lenk, JJ.

Cellular Telephone. Constitutional Law, Search and seizure, Probable cause, State action, Retroactivity of judicial holding. Search and Seizure, Expectation of privacy, Probable cause, Warrant. Probable Cause. Retroactivity of Judicial Holding. Evidence, Business record. Practice, Criminal, Warrant, Retroactivity of judicial holding.

Indictment found and returned in the Superior Court Department on July 29, 2011.

A pretrial motion to suppress evidence was heard by Janet L. Sanders, J.

An application for leave to file an interlocutory appeal was allowed by Gants, J., in the Supreme Judicial Court for the county of Suffolk.

Cailin M. Campbell, Assistant District Attorney, for the Commonwealth.

Matthew R. Segal (Jessie J. Rossman with him) for the defendant.

Hanni M. Fakhoury, of California, & Kit Walsh, for Electronic Frontier Foundation, amicus curiae, submitted a brief.

Matthew J. Tokson, of the District of Columbia, Elizabeth A. Lunt, Alex G. Philipson, Louis W. Tompros, Kevin S. Prussia, & Thaila K. Sundaresan, for Massachusetts Association of Criminal Defense Lawyers, amicus curiae, submitted a brief.

BOTSFORD, J. The central question we address in this appeal

is whether, consistent with the Massachusetts Constitution, the Commonwealth may obtain from a cellular telephone service provider (cellular service provider) historical cell site location information (CSLI)[1] for a particular cellular telephone without first obtaining a search warrant supported by probable cause. The Commonwealth appeals pursuant to Mass. R. Crim. P. 15 (a) (2), as appearing in 422 Mass. 1501 (1996), from an order of a judge in the Superior Court granting the defendant's motion to suppress evidence of CSLI associated with the cellular telephone he was using. The judge concluded that, although the Commonwealth had obtained the CSLI from the defendant's cellular service provider pursuant to a valid Superior Court order issued under 18 U.S.C. § 2703(d) (2006) of the Federal Stored Communications Act (SCA), the Commonwealth's access to the CSLI constituted a search within the meaning of art. 14 of the Massachusetts Declaration of Rights,[2] and therefore a search

---

[1] The term "cell site location information" (CSLI) refers to a cellular telephone service record or records that contain "information identifying the base station towers and sectors that receive transmissions from a [cellular] telephone." In re Application of the U.S. for an Order Authorizing the Release of Historical Cell Site Info., 736 F. Supp. 2d 578, 579 n.1 (E.D.N.Y. 2010) (In re Application for an Order I). "Historical" CSLI refers to CSLI relating to and generated by cellular telephone use that has "already occurred at the time of the order authorizing the disclosure of such data." Id. See In re Application of the U.S. for an Order Directing a Provider of Elec. Communication Serv. to Disclose Records to the Gov't, 620 F.3d 304, 308 (3d Cir. 2010).

[2] Article 14 of the Massachusetts Declaration of Rights provides:

"Every subject has a right to be secure from all

warrant based on probable cause was required.

On appeal, the Commonwealth principally asserts that no search in the constitutional sense occurred because CSLI is a business record of the defendant's cellular service provider, a private third party, and the defendant can have no expectation of privacy in location information -- i.e., information about the subscriber's location when using the cellular telephone -- that he voluntarily revealed. We conclude, like the motion judge, that although the CSLI at issue here is a business record of the defendant's cellular service provider, he had a reasonable expectation of privacy in it, and in the circumstances of this case -- where the CSLI obtained covered a two-week period -- the warrant requirement of art. 14 applies. We remand the case to the Superior Court, where the Commonwealth may seek to establish that the affidavit submitted in support of its application for an order under 18 U.S.C. § 2703(d) demonstrated probable cause for the CSLI records at issue.

1. Background. On the evening of August 24, 2004, Julaine Jules left her workplace and was not seen alive thereafter. Her body was recovered from the Charles River on September 19, 2004,

---

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."

and a criminal investigation into the death commenced.[3]

Early in the investigation, police became aware of the defendant, who had been a boy friend of Jules. State police Troopers Mary McCauley and Pi Heseltine interviewed the defendant in his home on August 28, 2004. In addition, Trooper McCauley obtained copies of telephone "call logs" for the defendant's and Jules's cellular telephones that included the date, time, duration, and telephone numbers of outgoing and incoming calls on August 24 and 25, 2004.[4]

On September 22, 2004, an assistant district attorney in Middlesex County filed in the Superior Court an application pursuant to 18 U.S.C. § 2703(c) of the SCA for an order under 18 U.S.C. § 2703(d) (§ 2703[d] order) to obtain from the defendant's cellular service provider, Sprint Spectrum (Sprint), certain records, including CSLI, associated with the cellular telephone used by the defendant;[5] the time period for which the records

---

[3] Because Julaine Jules's body was found on the Cambridge side of the Charles River, in Middlesex County, the district attorney for that county initiated the criminal investigation into her death. Based on evidence that incidents related to the possible crime had occurred in Suffolk County, the investigation was transferred to the office of the Suffolk County district attorney in late 2007 or early 2008.

[4] The record does not indicate by what means Trooper Mary McCauley obtained these telephone records, but it is reasonable to assume that the records were subpoenaed pursuant to G. L. c. 271, § 17B.

[5] The Commonwealth also appears to have sought an order to obtain similar CSLI records from Jules's cellular telephone service provider (cellular service provider), Cingular Wireless, for the same time period. That application, and any order that may have issued, are not included in the record here.

were sought appears to have been the fourteen-day period beginning August 24, 2004.[6] The Commonwealth's application for the § 2703(d) order was supported by an affidavit of Trooper McCauley, detailing her investigation and concluding that the records would be "important to show the general location" of the defendant and Jules on August 24 and 25 to "possibly include or exclude" the defendant "as a suspect."[7] A Superior Court judge

---

[6] The cellular telephone handset used by the defendant was obtained by Keisha Smith -- who was identified in Trooper McCauley's affidavit as another girl friend of the defendant -- for the defendant's exclusive use, and apparently Smith was the actual subscriber for the cellular telephone service with Sprint Spectrum (Sprint). The parties do not argue that Smith's role as owner of the telephone handset and cellular service subscriber has any bearing on the resolution of this case. They essentially treat the defendant as the owner and subscriber, and we do as well. This case is thus factually distinct from those in which a defendant has been found to be unable to demonstrate an expectation of privacy in his cellular telephone records because he used a fictitious name to obtain the cellular telephone service. See, e.g., United States vs. Wilson, U.S. Dist. Ct., No. 1:11-CR-53-TCB-ECS-3 (N.D. Ga. Feb. 20, 2013) (finding defendant lacked standing when no evidence linked him to false name on telephone account, which indicated "he [did] not want to be associated with it, or [was] trying to insulate himself from any responsibility for it").

[7] The order under 18 U.S.C. § 2703(d) (2006) (§ 2703[d] order) required the defendant's cellular service provider to turn over to authorities:

> "Any and all information . . . [regarding the defendant's cellular telephone number], for a 14 day period following and including August 24th, 2004, pertaining to both answered and unanswered calls . . . to destination and termination numbers which called or were called by the above telephone number on the above date, including but not limited to all connection logs and records of user activity for each such account, including but not limited to cell tower or site records, AMA Records, Roaming Table Requests, other information indicating the particular cell tower or site in which the subscriber's telephone handset was used or located, and other types of information that may be used to determine, or assist in

allowed the application, and the § 2703(d) order was issued the same day, September 22. It appears the Commonwealth received at least sixty-four pages of CSLI records relating to the defendant's cellular telephone.[8] Almost seven years later, on July 29, 2011, a Suffolk County grand jury indicted the defendant for the murder of Julaine Jules.[9]

On November 15, 2012, the defendant filed a motion to suppress evidence of his CSLI, which, he argued, was obtained in violation of his rights under the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights. After hearing, the motion judge allowed the defendant's motion,[10] concluding that "at least under art[.] 14 of the Massachusetts Declaration [of] Rights, there was a search such that this information must be suppressed."[11] The

---

determining, the physical location of the said telephone at the time of any of said calls (but not including any call or message content)."

The Commonwealth's actual application for the § 2703(d) order is not in the record before the court.

[8] The defendant represents, and the Commonwealth does not dispute, that the CSLI records provided to the Commonwealth by Sprint covered a period longer than the fourteen days stated in the § 2703(d) order, although the defendant has not indicated how much longer.

[9] The record contains no information relating to the seven-year interval between the commencement of the investigation into Jules's death and the indictment of the defendant.

[10] Also before the motion judge was a motion to suppress statements made by the defendant; that motion is not before us.

[11] The CSLI records at issue were not introduced at the motion hearing; the parties agreed at that time that the argument

Commonwealth filed an application for interlocutory review pursuant to Mass. R. Crim. P. 15 (a) (2) and G. L. c. 278, § 28E, which a single justice allowed and ordered to proceed before this court.[12]

2. Statutory scheme. The SCA, 18 U.S.C. § 2701 et seq. (2006 & Supp. III 2009), was enacted in 1986 as Title II of the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986). The SCA directs how governmental entities may obtain communication records from third-party providers of electronic communication services. See In re Application of the U.S. for an Order Directing a Provider of Elec. Communication Serv. to Disclose Records to the Gov't, 620 F.3d 304, 306 (3d Cir. 2010). The purpose of the SCA was "to protect the privacy of users of electronic communications by criminalizing the unauthorized access of the contents and transactional records of stored wire and electronic communications, while providing an avenue for law enforcement entities to compel a provider of

---

on the motion was "essentially a legal argument" and that an evidentiary hearing was unnecessary.

[12] Following oral argument in this case, this court, taking the view that a review of the CSLI obtained pursuant to the § 2703(d) order might assist our understanding and consideration of the issues raised, requested that the Commonwealth produce the CSLI records. The Commonwealth objected, and a single justice held a hearing on the question whether the appellate record should be expanded to include the CSLI evidence. Based on the information about the CSLI records that the parties provided at that hearing, and in light of the Commonwealth's objection, we will not expand the record, having determined that a review of the CSLI evidence is not essential to resolution of the issues before us.

electronic communication services to disclose the contents and records of electronic communications." In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 707 F.3d 283, 286-287 (4th Cir. 2013).

At issue here is 18 U.S.C. § 2703, which governs the compelled disclosure of customer communications or records to a governmental entity, and in particular, 18 U.S.C. §§ 2703(c)(1)(B) and (d). Section 2703(c)(1)(B)[13] authorizes a governmental entity to require an electronic communication provider, such as a cellular telephone service company, to disclose communication records (not including the contents) for a particular customer if the government obtains a court order pursuant to § 2703(d). Section 2703(d), in turn, specifies:

> "A court order for disclosure . . . 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 . . . records or other information sought, are relevant and material to an ongoing criminal investigation" (emphases added).

The standard required for a § 2703(d) order thus is less than

---

[13] This section provides in pertinent part:

> "(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 --
>
> ". . .
>
> "(B) obtains a court order for such disclosure under subsection (d) of this section . . . ."

probable cause, see, e.g., In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 606 (5th Cir. 2013); it is "essentially a reasonable suspicion standard." In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 707 F.3d at 287.

The parties agree that the SCA applies to the CSLI in this case,[14] and that the § 2703(d) order issued by the Superior Court judge was valid insofar as it was based on a showing of "specific and articulable facts showing that there are reasonable grounds to believe" that the CSLI records sought were "relevant and material to an ongoing criminal investigation," 18 U.S.C. § 2703(d). They disagree, however, about whether this statutory standard is constitutionally sufficient. Stated otherwise, the parties dispute whether, under the Fourth Amendment or art. 14, the Commonwealth may obtain the CSLI from a cellular service provider solely on the basis of a § 2703(d) order, or may only do so by obtaining a search warrant based on probable cause.[15]

---

[14] See United States v. Graham, 846 F. Supp. 2d 384, 396 (D. Md. 2012) (§ 2703[c][1][B] applies to historical cell site location data, thereby permitting government to seek such data pursuant to order issued under § 2703[d]); In re Applications of the U.S. for Orders Pursuant to 18 U.S.C. § 2703(d), 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

[15] As in the context of location tracking through the use of global positioning system (GPS) technology, "probable cause" in the context of CSLI means "probable cause to believe that a particularly described offense has been . . . committed" and that the CSLI sought will "produce evidence of such offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed . . . such offense." See Commonwealth v. Connolly, 454 Mass. 808, 825 (2009).

3. Cellular telephone technology. A brief explanation of cellular telephone technology informs our discussion of the issues raised. The basic facts about how a cellular telephone works and how a cellular service provider keeps CSLI records are not in dispute.[16] A cellular telephone communicates with the telephone network via radio waves. ECPA (Part II): Geolocation Privacy and Surveillance: Hearing Before the H. Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary, 113th Cong. 50 (2013) (testimony of Professor Matt Blaze) (Blaze Testimony II). See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 20 (2010) (testimony of Professor Matt Blaze) (Blaze Testimony I).[17] A cellular service provider has a network of base

---

[16] This case concerns CSLI and cellular telephone technology from 2004 and a specific request for CSLI that produced a specific record response. While we decide this case based on the record before us, we have not restricted our analysis of the constitutional issues raised to the state of cellular telephone technology as it may have existed in 2004. See Kyllo v. United States, 533 U.S. 27, 36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development"); State v. Earls, 214 N.J. 564, 587 (N.J. 2013) (considering technology of older cellular telephone and noting "[w]e are not able to draw a fine line across that spectrum and calculate a person's legitimate expectation of privacy with mathematical certainty -- noting each slight forward advance in technology. Courts are not adept at that task").

[17] The Commonwealth references Professor Matt Blaze's 2010 and 2013 congressional testimony in its brief, and the defendant references the 2013 testimony.

stations, also referred to as cell sites or cell towers, that essentially divides the provider's service area into "sectors." Blaze Testimony II, supra at 43, 53. Cell site antennae send and receive signals from subscribers' cellular telephones that are operating within a particular sector. In re Applications of the U.S. for Orders Pursuant to 18 U.S.C. § 2703(d), 509 F. Supp. 2d 76, 78 (D. Mass. 2007). Additionally, if a subscriber begins a call connected to a particular cell site and then moves closer to a different one, the call is automatically "handed off" to that closer cell site. Blaze Testimony I, supra at 20. When a subscriber makes or receives a call, the cellular service provider records the identity of the cell site utilized.[18,19]

---

[18] Additionally, when they are "powered on," cellular telephones regularly identify themselves to the nearest cell site with the strongest signal, through a process known as "registration." Registration is automatic, occurring every seven seconds. See In re Application for Pen Register & Trap/Trace Device with Cell Cite Location Auth., 396 F. Supp. 2d 747, 750-751 (S.D. Tex. 2005); ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 20 (2010) (testimony of Professor Matt Blaze) (Blaze Testimony I).

[19] While data collection and record retention practices vary among cellular service providers, companies "typically create 'call detail records' that can include the most accurate location information available to them." ECPA (Part II): Geolocation Privacy and Surveillance: Hearing Before the H. Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary, 113th Cong. 57 (2013) (testimony of Professor Matt Blaze) (Blaze Testimony II). For a number of years, cellular service providers' call records have routinely included the identity of the cell sector that handled a particular call. Id. Currently, records may include even more detailed information such as registration data or the cellular telephone user's latitude and longitude. Id.

Blaze Testimony II, supra at 53. Through such "network-based location techniques," a cellular service provider can approximate the location of any active cellular telephone handset within its network based on the handset's communication with a particular cell site.[20] Id. at 52-53.[21]

As cellular telephone use has grown, cellular service providers have responded by adding new cell sites to accommodate additional customers. Id. at 54. See Blaze Testimony I, supra at 24. The number of cell sites in the United States has risen from 139,338 in 2002 to 301,779 in 2012, a more than twofold increase. See CTIA: The Wireless Association, Wireless Quick Facts (Nov. 2013), http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts (last viewed Feb. 14, 2014)

---

[20] See Earls, 214 N.J. at 577, quoting Blaze Testimony I, supra, and citing Pell & Soghoian, Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact, 27 Berkeley Tech. L.J. 117 (2012) (Pell & Soghoian):

> "Network-based location tracking relies on the network of cell sites and antennas . . . . As mobile devices register with a cell site, make a call, or download data, they 'communicate' with a station through radio signal data that is collected and analyzed at the provider's cell towers. [Blaze Testimony I, supra] at 22. That process enables carriers to identify 'the position of virtually every handset active in the network at all times.' [Id.] The information is typically created and stored in a database. Id. at 27. A log is also ordinarily created each time a call is made or data downloaded. [Id.] Pell & Soghoian, [supra] at 128."

[21] The other way that the location of a cellular telephone can be tracked is through built-in GPS satellite receiver hardware that enables a cellular telephone to track its own location. Blaze Testimony II, supra at 51. This type of location tracking is not at issue here.

(CTIA Wireless Quick Facts). When new cell sites are created, existing sectors become smaller, which, in turn, makes network-based location tracking increasingly accurate. Blaze Testimony I, supra at 25.[22,23] See Blaze Testimony II, supra at 55 ("The effect of this trend toward smaller cell sectors is that knowing the identity of the base station . . . that handled a call is tantamount to knowing a [tele]phone's location to within a relatively small geographic area").

In the present case, while the CSLI obtained by the Commonwealth is not in the record, the Commonwealth has provided a description of it that the defendant appears to accept. The CSLI that the Commonwealth received from Sprint includes, for a two-week period (or somewhat longer, see note 8, supra) beginning August 24, 2004, the telephone numbers, the date and time, and the numbers of the cell sites used for all the calls made and

---

[22] Moreover, because cellular telephone users expect their telephones to "do more and to work in more locations," increased pressure is placed on individual cell sites, each of which has "a limited number of calls that it can process" and "a limited number of data services that it can handle simultaneously from different customers." Blaze Testimony II, supra at 43, 54. "So as cellular . . . technology has grown and become so important, as we all get different mobile devices and use them more often for more things, with higher bandwidth broadband connections, service providers have had no choice but to reduce the geographic area over which each base station operates so that smaller cell towers, smaller antennas cover a smaller number of users . . . ." Id. at 43.

[23] In addition, cellular service providers are now capable of "triangulating" signals from multiple towers, which "substantially enhance[es]" the precision of location data. In re Smartphone Geolocation Data Application, U.S. Dist. Ct., No. 13-MJ-242 GRB (E.D.N.Y. May 1, 2013).

received by the defendant's cellular telephone handset -- including, we infer from the § 2703(d) order, unanswered calls -- as well as the latitude and longitude of the cell sites to which those calls connected in order to conduct those calls. SMS or short message service messages (text messages), Internet use, or any type of "registration" (see note 18, supra) or "triangulated" (see note 23, supra) data are not included.[24]

4. Discussion. In its appeal, the Commonwealth raises three arguments: (1) if a search took place in this case, the defendant has not met his burden to show it involved State action; (2) the defendant has not established that, in fact, a search in the constitutional sense did take place, because he has no reasonable expectation of privacy in the Sprint CSLI records; and (3) if the court nonetheless concludes that the Commonwealth's obtaining the CSLI did constitute a search in the constitutional sense and required a warrant, the exclusionary rule should not apply. We consider each argument in turn.

a. State action. The Commonwealth contends that there was no State action here because the Commonwealth played no role in

---

[24] As indicated in the text, the CSLI sought by the Commonwealth and at issue here is "historical" CSLI, meaning the calls already have occurred when the data are requested. CSLI also can be "prospective," a term that refers to location data that will be generated sometime after the order authorizing its disclosure. In re Application for an Order I, 736 F. Supp. 2d at 579 n.1. The privacy interest raised by historical CSLI may be the same as prospective, or "real-time," CSLI. See id. at 585. But see In re Applications of the U.S. for Orders Pursuant to 18 U.S.C. § 2703(d), 509 F. Supp. 2d at 81 (distinguishing between real-time and historical CSLI). However, we do not need to consider that question in the present case.

collecting the CSLI at issue: the data were captured or collected by Sprint on its own and already existed before the Commonwealth became involved in the case. The argument fails.

The Commonwealth is correct that the protections against unreasonable searches afforded by the Fourth Amendment and art. 14 are only implicated when a search or seizure is "conducted by or at the direction of the State." District Attorney for the Plymouth Dist. v. Coffey, 386 Mass. 218, 220-221 (1982). "Evidence discovered and seized by private parties is admissible without regard to the methods used, unless State officials have instigated or participated in the search." Commonwealth v. Brandwein, 435 Mass. 623, 632 (2002), quoting Commonwealth v. Leone, 386 Mass. 329, 333 (1982). Accordingly, our cases have held consistently that there is no State action when information is disclosed voluntarily to the government by a private party. See, e.g., Commonwealth v. Rivera, 445 Mass. 119, 124 (2005) (denying motion to suppress when "police had no part in making, inducing, soliciting, or otherwise encouraging or abetting the making of the surveillance tape. The tape . . . fell into their hands"); Brandwein, supra at 631 (given that individuals "volunteered information concerning the defendant's involvement in criminal activity" to police, "[n]othing in our law prevented [police] from acting on that information").

It is altogether different, however, where the government compels a private party to produce and provide to it personal information about a person. On this point, the Commonwealth's

reliance on Coffey, 386 Mass. at 218, is misplaced. In that case, a woman who was receiving harassing calls asked her telephone company to install a cross frame unit trap on her telephone line to determine the source of the incoming calls. Id. at 219. The court found "no evidence . . . of any relationship between the telephone company and the State" and concluded that "a finding of State action [was] not warranted," id. at 222, because the Commonwealth was not involved in placing the trap on the telephone. The Commonwealth makes much of the fact that in Coffey, as here, the government was not actually involved in collecting the data. But the Commonwealth overlooks the critical point that in Coffey, the subscriber requested that the telephone company put a trap on her telephone line and the telephone company appears to have volunteered to turn the resulting information over to the Commonwealth. Id. at 219. Here, in contrast, through a court order, the Commonwealth compelled Sprint to turn over the defendant's CSLI. Because the § 2703(d) order required the CSLI disclosure and a search was "instigated" by the Commonwealth, State action clearly was involved. See Brandwein, 435 Mass. at 632. The defendant has met his burden to show that the search was conducted by or at the direction of the State.

b. The defendant's reasonable expectation of privacy. Under both the Federal and Massachusetts Constitutions, a search in the constitutional sense occurs when the government's conduct intrudes on a person's reasonable expectation of privacy. Katz

v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (intrusion into area where person has reasonable expectation of privacy may violate Fourth Amendment). Commonwealth v. Montanez, 410 Mass. 290, 301 (1991) (articulating same standard under art. 14). "The measure of the defendant's expectation of privacy 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, supra. See Katz, supra (Harlan, J., concurring); Commonwealth v. Blood, 400 Mass. 61, 68 (1987).

There is no dispute that if the CSLI were a personal record belonging to the defendant and in his possession, the Commonwealth would have no right to obtain it without complying with the warrant requirements of the Fourth Amendment and art. 14. The Commonwealth anchors its argument in the third-party doctrine adopted by the United States Supreme Court in relation to the Fourth Amendment and in certain circumstances applied by this court in relation to art. 14. If the Commonwealth is correct, then it did not need to obtain a warrant here and was entitled to obtain the CSLI from Sprint pursuant to the § 2703(d) order alone. We turn, therefore, to the third-party doctrine.

The doctrine has its roots in a pair of United States Supreme Court cases that predate cellular telephones. In United States v. Miller, 425 U.S. 435, 438-440 (1976), the Court considered whether the defendant had a Fourth Amendment privacy

interest in his bank records, including his checks, deposit slips, and monthly statements. Reasoning that the documents were "business records of the banks," the Court "perceive[d] no legitimate 'expectation of privacy' in their contents." Id. at 440, 442. Specifically, the records contained information "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," id. at 442, and therefore "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." Id. at 443. The Court concluded:

> "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

Id.

Smith v. Maryland, 442 U.S. 735, 737, 742 (1979), presented the question whether the defendant had a legitimate expectation of privacy in the telephone numbers that he dialed on his home telephone. The telephone company, at police request, had installed a pen register -- a mechanical device that records the telephone numbers dialed on a particular telephone -- in order to capture information about the defendant Smith's call history. Id. at 736 n.1, 737. Reasoning that "[t]elephone users . . . typically know that they must convey numerical information to the [telephone] company; that the [telephone] company has facilities for recording this information; and that the [telephone] company

does in fact record this information for a variety of legitimate business purposes," the Court rejected the notion that telephone subscribers "harbor any general expectation that the numbers they dial will remain secret." Id. at 743. Applying the reasoning of Miller, 425 U.S. at 442-443, the Court stated that, "[w]hen he used his [telephone], [the defendant] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [the defendant] assumed the risk that the company would reveal to police the numbers he dialed." Smith, supra at 744.

Although the Supreme Court has not considered the issue whether the government's obtaining CSLI from a cellular service provider constitutes a search in the constitutional sense, a number of lower Federal courts have done so. Applying the third-party doctrine articulated in Miller and Smith, a majority of these courts has ruled that an individual has no reasonable expectation of privacy in the CSLI because it is a third-party business record, and therefore the warrant requirement of the Fourth Amendment does not apply.[25] Some Federal courts, however,

---

[25] See, e.g., In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 611-615 (5th Cir. 2013); Graham, 846 F. Supp. 2d at 398; United States vs. Rigmaiden, U.S. Dist. Ct., No. CR 08-814-PHX-DGC (D. Ariz. May 8, 2013); United States vs. Ruby, U.S. Dist. Ct., No. 12CR1073 WQH (S.D. Cal. Feb. 12, 2013); United States vs. Madison, U.S. Dist. Ct., No. 11-60285-CR (S.D. Fla. July 30, 2012); United States vs. Dye, U.S. Dist. Ct., No. 1:10CR221 (N.D. Ohio Apr. 27, 2011), aff'd, 538 Fed. Appx. 654 (6th Cir. 2013); United States vs. Velasquez, U.S. Dist. Ct., No. CR 08-0730 WHA (N.D. Cal. Oct. 22, 2010); United States vs.

have come to the opposite conclusion.[26] We have no need to wade into these Fourth Amendment waters and focus instead on the third-party doctrine in relation to art. 14.

In earlier cases considering a person's reasonable expectation of privacy in third-party telephone records under art. 14, this court essentially tracked Fourth Amendment jurisprudence, and applied in substance the Supreme Court's third-party doctrine. See Commonwealth v. Vinnie, 428 Mass. 161, 178, cert. denied, 525 U.S. 1007 (1998) (no reasonable expectation of privacy under art. 14 in telephone billing records and therefore search warrant not required; records may be obtained under G. L. c. 271, § 17B, by administrative subpoena on "reasonable grounds for belief" of telephone's use for "unlawful purpose");[27] Commonwealth v. Cote, 407 Mass. 827, 834-836 (1990) (no reasonable expectation of privacy under Fourth Amendment or art. 14 in telephone answering service message records). However, "[w]e have often recognized that art. 14 . . . does, or may, afford more substantive protection to individuals than that which prevails under the Constitution of the United States."

Suarez-Blanca, U.S. Dist. Ct., No. 1:07-CR-0023-MHS/AJB (N.D. Ga. Apr. 21, 2008); United States vs. Benford, U.S. Dist. Ct., No. 2:09 CR 86 (N.D. Ind. Mar. 26, 2010).

[26] See, e.g., In re Application of the U.S. for an Order Authorizing the Release of Historical Cell Site Info., 809 F. Supp. 2d 113, 120-126 (E.D.N.Y. 2011) (In re Application for an Order II); In re Application for an Order I, 736 F. Supp. 2d at 588-589.

[27] In Commonwealth v. Feodoroff, 43 Mass. App. Ct. 725, 729-730 (1997), the Appeals Court had reached the same conclusion.

Blood, 400 Mass. at 68 n.9. And we have specifically indicated that this may be so in relation to third-party records. See, e.g., Commonwealth v. Buccella, 434 Mass. 473, 484 n.9 (2001), cert. denied, 534 U.S. 1079 (2002) (recognizing that "analysis of an expectation of privacy following entrustment to a third party might be different under art. 14"); Cote, supra at 835 ("It may be that under art. 14 exposure of information to another party might not compel the rejection of a claim of a reasonable expectation of privacy"). In the present case, the possibility mentioned in Buccella and Cote is the one we must consider: whether, notwithstanding that the CSLI is a business record of the defendant's cellular service provider, the defendant has a reasonable expectation of privacy in it that is recognized and protected by art. 14.

The Commonwealth would answer no. As previously stated, in the Commonwealth's view, the third-party doctrine applies to defeat the defendant's claim, because like the defendant in Smith, 442 U.S. at 744, the defendant here can have no reasonable expectation of privacy in a cellular service provider's CSLI records that simply reflect information he supplied voluntarily by choosing to use his cellular telephone. We agree with the defendant, however, that the nature of cellular telephone technology and CSLI and the character of cellular telephone use in our current society render the third-party doctrine of Miller and Smith inapposite; the digital age has altered dramatically the societal landscape from the 1970s, when Miller and Smith were

written.

Considering first cellular telephone use, like other courts, we recognize that the cellular telephone has become "an indispensable part of modern [American] life." State v. Earls, 214 N.J. 564, 586 (2013). See United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in the judgment) (noting that, as of June, 2011, "there were more than 322 million wireless devices in use in the United States"); CTIA Wireless Quick Facts, supra (reporting that, as of December, 2012, there were more than 326 million wireless subscriber connections in United States). Further, "[m]any households now forgo traditional 'landline' telephone service, opting instead for cellular phones carried by each family member." Blaze Testimony II, supra at 48. See CTIA Wireless Quick Facts, supra (noting that, as of December, 2012, over 38 per cent of all American households were "wireless-only").

Indeed, cellular telephones are increasingly viewed as necessary to social interactions as well as the conduct of business.[28] More fundamentally, and of obvious importance to the present case, cellular telephones physically accompany their

---

[28] See Blaze Testimony II, supra at 48:

> "There is perhaps no more ubiquitous symbol of our highly connected society than the cellular telephone. Over the course of only a few short decades, mobile communication devices have evolved from being little more than an expensive curiosity for the wealthy into a basic necessity for most Americans, transforming the way we communicate with one another, do business, and obtain and manage the increasing volume of information that is available to us."

users everywhere -- almost permanent attachments to their bodies. See 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) (In re Application for an Order II) ("For many Americans, there is no time in the day when they are more than a few feet away from their [cellular telephones]"). As anyone knows who has walked down the street or taken public transportation in a city like Boston, many if not most of one's fellow pedestrians or travelers are constantly using their cellular telephones[29] as they walk or ride -- as the facts of this case appear to illustrate.[30] As people do so, they are constantly connecting to cell sites, and those connections are recorded as CSLI by their cellular service providers.

Turning, then, to the nature or function of CSLI, there is no question that it tracks the location of a cellular telephone

---

[29] In 2012, there were 2.3 trillion voice minutes of use on wireless devices such as cellular telephones in the United States; in 2007, the comparable annual figure was 2.12 trillion, and in 1997, it was 62.9 billion. CTIA: The Wireless Association, Wireless Quick Facts (Nov. 2013), http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts (last viewed Feb. 14, 2014) (CTIA Wireless Quick Facts). As for short message service messages (text messages), there were 2.19 trillion messages sent in 2012; and in 2007, the annual figure was 362.5 billion. Id. (no information about text message use in 1997 was included).

[30] The record indicates that the defendant was engaged in a telephone call for ninety-one consecutive minutes, and according to information contained in Trooper McCauley's affidavit, while he was so engaged, he was traveling from Sullivan Square in Charlestown to the Haymarket area in Boston, to a Massachusetts Bay Transportation Authority station in the Dorchester area of Boston, and then to his home in Dorchester.

user, which is the reason the Commonwealth is interested in obtaining it.[31] Clearly, tracking a person's movements implicates privacy concerns. In Commonwealth v. Rousseau, 465 Mass. 372 (2013), a case involving global positioning system (GPS) tracking of a defendant's vehicle by the Commonwealth, we focused on this point. We noted that in Jones, 132 S. Ct. at 955, 964, five Justices of the United States Supreme Court concluded that GPS tracking of a vehicle, at least for more than a short period of time, intruded on an individual's reasonable

---

[31] The motion judge focused in her opinion on the similarity between CSLI and GPS data in terms of the ability to track an individual's location. The Commonwealth argues at length that this was error because there is no evidence in the record of the relative degree of accuracy of CSLI as compared to GPS data, and that the comparative accuracy of location identification, or even the accuracy of location identification on its own, is not the type of fact of which the judge could take judicial notice. In particular, it objects to the finding that over time the difference between CSLI and GPS data has "diminished," such that "CSLI is now no less accurate than GPS in pinpointing location." We find it unnecessary to consider this argument because whatever the specific facts about the relative precision of GPS data and the CSLI at issue here, the Commonwealth agrees that CSLI does track location and that, as indicated in the text, it seeks the CSLI precisely because of its location-tracking abilities. See, e.g., Connolly, 454 Mass. at 835 (Gants, J., concurring) ("Even without GPS technology, any cellular telephone, when it is turned on, can be traced to the tower with which it is communicating, giving an approximate location"); In re Application for an Order I, 736 F. Supp. 2d at 591 (noting that only reason government seeks CSLI is that it believes CSLI "will provide meaningful information about [defendant's] past movements"). Moreover, as the congressional testimony of Professor Blaze indicates, although the precision of CSLI may vary among cellular service providers, with the profusion of new cell sites, particularly in urban areas such as in this case, CSLI has become increasingly precise in identifying the location of a cellular telephone user at any point in time. Blaze Testimony II, supra at 59.

expectation of privacy, and we agreed.[32] Rousseau, supra at 381-382. We stated,

> "[T]he government's contemporaneous electronic monitoring of one's comings and goings in public places invades one's reasonable expectation of privacy. We conclude that under art. 14, a person may reasonably expect not to be subjected to extended GPS electronic surveillance by the government, targeted at his movements, without judicial oversight and a showing of probable cause."

Id. at 382. See Jones, supra at 954-955 (Sotomayor, J., concurring); Commonwealth v. Connolly, 454 Mass. 808, 833-835 (2009) (Gants, J., concurring); People v. Weaver, 12 N.Y.3d 433,

---

[32] In United States v. Jones, 132 S. Ct. 945, 948 (2012), the Court considered whether law enforcement officers' attachment of a GPS tracking device to the defendant's vehicle in order to monitor its movement was a search within the meaning of the Fourth Amendment. Pointing to the officers' physical intrusion into the vehicle in order to install the device and applying a property-based common-law trespass theory, five Justices concluded that a search in the constitutional sense had occurred. Id. at 949. The majority also stated that, while not present on these facts, "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy." Id. at 954. In concurrence, Justice Alito rejected the majority's trespass theory, concluding instead that:

> "[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. . . . But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not -- and indeed, in the main, simply could not -- secretly monitor and catalogue every single movement of an individual's car for a very long period."

Id. at 964 (Alito, J., concurring in the judgment). Three Justices joined in this concurrence, and Justice Sotomayor, in a separate concurring opinion, joined in Justice Alito's view about privacy. See id. at 955 (Sotomayor, J., concurring) (agreeing that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy").

444-447 (2009).

It is evident that CSLI implicates the same nature of privacy concerns as a GPS tracking device. As the New Jersey Supreme Court stated:

> "Using a [cellular telephone] to determine the location of its owner can be far more revealing than acquiring toll billing, bank, or Internet subscriber records. It is akin to using a tracking device and can function as a substitute for 24/7 surveillance without police having to confront the limits of their resources. It also involves a degree of intrusion that a reasonable person would not anticipate. . . . Location information gleaned from a [cellular telephone] provider can reveal not just where people go -- which doctors, religious services, and stores they visit -- but also the people and groups they choose to affiliate with and when they actually do so. That information cuts across a broad range of personal ties with family, friends, political groups, health care providers, and others. . . . In other words, details about the location of a [cellular telephone] can provide an intimate picture of one's daily life." (Citations omitted.)

Earls, 214 N.J. at 586.[33]

Indeed, as the defendant contends, because of the nature of cellular telephone use and technology, there is a strong argument that CSLI raises even greater privacy concerns than a GPS

---

[33] Observations of Justice Sotomayor concerning GPS tracking by the government in Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring), have particular resonance in relation to the government's acquisition of CSLI:

> "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring -- by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track -- may 'alter the relationship between citizen and government in a way that is inimical to democratic society'" (citation omitted).

tracking device. In contrast to such a device attached to a vehicle, see, e.g., Rousseau, 465 Mass. at 374; Connolly, 454 Mass. at 810, because a cellular telephone is carried on the person of its user, it tracks the user's location far beyond the limitations of where a car can travel. See, e.g., United States vs. Powell, U.S. Dist. Ct., No. 12-cr-20052 (E.D. Mich. May 3, 2013) ("There are practical limits on where a GPS tracking device attached [to] a person's vehicle may go. A [cellular telephone], on the other hand, is usually carried with a person wherever they go"). As a result, CSLI clearly has the potential to track a cellular telephone user's location in constitutionally protected areas.

We return to the third-party doctrine. As discussed, the Supreme Court has identified the central premise of the doctrine -- at least as applied to records held by a third-party telephone company -- to be that when one voluntarily conveys information to the company, such as the telephone numbers one is dialing, and knows that the company records this information for legitimate business purposes, one assumes the risk that the company will disclose that information to others, including the government. See Smith, 442 U.S. at 743-744. In other words, in these circumstances, no expectation of privacy would be reasonable. The dissent here argues that at least where the CSLI obtained by the government is limited, as in this case, to location information relating to telephone calls made and received (whether answered or not), the third-party doctrine still fits;

the dissent sees "no principled reason" why the third-party doctrine should apply to the telephone numbers recorded in the pen register in Smith but not to this location information. Post at .

We find a significant difference between the two. In Smith, the information and related record sought by the government, namely, the record of telephone numbers dialed, was exactly the same information that the telephone subscriber had knowingly provided to the telephone company when he took the affirmative step of dialing the calls. The information conveyed also was central to the subscriber's primary purpose for owning and using the cellular telephone: to communicate with others. No cellular telephone user, however, voluntarily conveys CSLI to his or her cellular service provider in the sense that he or she first identifies a discrete item of information or data point like a telephone number (or a check or deposit slip as in Miller, 425 U.S. at 442) and then transmits it to the provider. CSLI is purely a function and product of cellular telephone technology, created by the provider's system network at the time that a cellular telephone call connects to a cell site. And at least with respect to calls received but not answered, this information would be unknown and unknowable to the telephone user in advance -- or probably at any time until he or she receives a copy of the CSLI record itself.[34] Moreover, it is of course the case that

---

[34] The defendant argues in part that a person like him using a cellular telephone is not even aware that the cellular service

CSLI has no connection at all to the reason people use cellular telephones. See Earls, 214 N.J. at 587 ("People buy [cellular telephones] to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a [cellular telephone] to share detailed information about their whereabouts with the police"). Moreover, the government here is not seeking to obtain information provided to the cellular service provider by the defendant. Rather, it is looking only for the location-identifying by-product of the cellular telephone technology -- a serendipitous (but welcome) gift to law enforcement investigations. Finally, in terms of the privacy interest at stake here -- the individual's justifiable interest in not having "his comings and goings . . . continuously and contemporaneously monitored" by the government, see Connolly, 454

---

provider collects CSLI, and therefore cannot be said to convey such information voluntarily to the provider. Some courts have adopted similar reasoning. See, e.g., In re Application of the U.S. for an Order Directing a Provider of Elec. Communication Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317-318 (3d Cir. 2010). While this reasoning currently may resonate with many cellular telephone users, it ignores the reality of cellular telephone technology and the growing sophistication of such users in an increasingly digital age. See In re Application for an Order II, 809 F. Supp. 2d at 121 ("This definition [of voluntary sharing] relies too heavily on [cellular telephone] users remaining unaware of the capacities of cellular technology, a doubtful proposition in the first place. Public ignorance as to the existence of cell-site-location records, however, cannot long be maintained. Rather the expectation of privacy in cell-site-location records, if one exists, must be anchored in something more permanent -- it must exist despite the public's knowledge that these records are collected by their cellular service providers"). See also Henderson, Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search, 55 Cath. U. L. Rev. 373, 388 (2006).

Mass. at 835 (Gants, J., concurring) -- the enormous difference between the cellular telephone in this case and the "land line" telephone in Smith seems very relevant. In terms of location, a call log relating to a land line may indicate whether the subscriber is at home, but no more. But for a cellular telephone user carrying a telephone handset (as the defendant was), even CSLI limited to the cell site locations of telephone calls made and received may yield a treasure trove of very detailed and extensive information about the individual's "comings and goings" in both public and private places; in this case, as mentioned, the defendant's CSLI obtained by the Commonwealth covered at least sixty-four pages.

In sum, even though CSLI is business information belonging to and existing in the records of a private cellular service provider, it is substantively different from the types of information and records contemplated by Smith and Miller, the Supreme Court's seminal third-party doctrine cases. These differences lead us to conclude that for purposes of considering the application of art. 14 in this case, it would be inappropriate to apply the third-party doctrine to CSLI. This is not to say that under art. 14, the fact of a person's voluntary disclosure of otherwise private information to a third party is always irrelevant. In other words, we do not reject categorically the third-party doctrine and its principle that disclosure to a third party defeats an expectation of privacy, and we see no reason to change our view that the third-party

doctrine applies to traditional telephone records. See, e.g., Vinnie, 428 Mass. at 178; Cote, 407 Mass. at 834-835. However, all the distinctive characteristics of cellular telephone technology and CSLI that we have discussed require that we take a different approach with respect to CSLI.[35]

Having so concluded, the central question here remains to be answered: whether, given its capacity to track the movements of the cellular telephone user, CSLI implicates the defendant's privacy interests to the extent that under art. 14, the government must obtain a search warrant to obtain it. There is no real question that the government, without securing a warrant, may use electronic devices to monitor an individual's movements in public to the extent that the same result could be achieved through visual surveillance. See United States v. Knotts, 460 U.S. 276, 282, 285 (1983) (no Fourth Amendment violation when, without warrant, police used electronic tracking device to track defendant's movement on public roads). However,

---

[35] Although, as stated in the text, we do not reject the third-party doctrine as a general matter, the rapid expansion in the quantity of third-party data generated through new technologies raises important questions about the continued viability of the third-party doctrine in the digital age. See Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach 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" [citations omitted]). See Henderson, After United States v. Jones, After the Fourth Amendment Third Party Doctrine, 14 N.C. J. L. & Tech. 431, 435-436 (2013).

the Supreme Court has recognized as well that a different result may obtain when the monitoring involves a person's home because of the person's fundamental privacy interest attached to that location. See United States v. Karo, 468 U.S. 705, 714 (1984) (concluding that "the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence"). We similarly have recognized that the "sanctity of the home" warrants protection under art. 14: "all details [in the home] are intimate details, because the entire area is held safe from prying government eyes." Commonwealth v. Porter P., 456 Mass. 254, 260 (2010), quoting Kyllo v. United States, 533 U.S. 27, 37 (2001). This distinction between privacy interests in public and private spaces makes CSLI especially problematic, because cellular telephones give off signals from within both 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. See Earls, 214 N.J. at 586. See also United States vs. Powell, No. 12-cr-20052 ("If at any point a tracked [cellular telephone] signaled that it was inside a private residence . . . , 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"). Given that art. 14 protects against warrantless intrusion into private places, we cannot ignore the

probability that, as CSLI becomes more precise, cellular telephone users will be tracked in constitutionally protected areas.

Considering GPS vehicle location tracking, a number of courts -- including this court -- have determined that it is only when such tracking takes place over extended periods of time that the cumulative nature of the information collected implicates a privacy interest on the part of the individual who is the target of the tracking. See Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring); id. at 964 (Alito, J., concurring); United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), aff'd sub nom. United States v. Jones, 132 S. Ct. 945 (2012); Rousseau, 465 Mass. at 382. This rationale has been extended to the context of CSLI. See, e.g., In re Application for an Order II, 809 F. Supp. 2d at 122; In re Application of the U.S. for an Order Authorizing the Release of Historical Cell Site Info., 736 F. Supp. 2d 578, 590 (E.D.N.Y. 2010). See also In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., U.S. Dist. Ct., No. 11-MC-0113 (E.D.N.Y. Feb. 16, 2011) (discussing "length of time over which location tracking technology must be sustained to trigger the warrant requirement" and recognizing that "any such line-drawing is, at least to some extent, arbitrary, and that the need for such arbitrariness arguably undermines the persuasiveness of the rationale of Maynard," but ultimately concluding that length of tracking matters to constitutional analysis).

The motion judge, however, ruled that the length of time over which the historical CSLI is collected is not relevant to an assessment of a subscriber's privacy interest in this information. Her view finds some support in the differences between the two types of tracking represented by GPS data and historical CSLI. In particular, at the core of the courts' reasoning in both Jones, 132 S. Ct. at 964 (Alito, J., concurring), and Rousseau, supra at 381-382, is that prospective, short-term GPS vehicle tracking by the government is similar to visual surveillance, a traditional law enforcement tool that does not implicate constitutionally protected privacy interests. See Knotts, 460 U.S. at 282, 285. But, as the motion judge observed, when the government obtains historical CSLI from a cellular service provider, the government is able to track and reconstruct a person's past movements, a category of information that never would be available through the use of traditional law enforcement tools of investigation. Furthermore, as discussed previously, cellular telephone location tracking and the creation of CSLI can indeed be more intrusive than GPS vehicle tracking.

We recognize this difference between GPS vehicle location tracking and historical CSLI. Nonetheless, we also recognize that in terms of the constitutional question raised, GPS data and historical CSLI are linked at a fundamental level: they both implicate the same constitutionally protected interest -- a person's reasonable expectation of privacy -- in the same manner

-- by tracking the person's movements.[36] Given this intrinsic link, it is likely that the duration of the period for which historical CSLI is sought will be a relevant consideration in the reasonable expectation of privacy calculus -- that there is 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. But there is no need to consider at this juncture what the boundaries of such a time period might be in this case because, for all the reasons previously rehearsed concerning the extent and character of cellular telephone use, the two weeks covered by the § 2703(d) order at issue exceeds it: even though restricted to telephone calls sent and received (answered or unanswered), the tracking of the defendant's movements in the urban Boston area for two weeks was more than sufficient to intrude upon the defendant's expectation of privacy safeguarded by art. 14.[37] Cf. Rousseau,

---

[36] The link between prospective CSLI and GPS location tracking would appear to be even stronger than is true of historical CSLI, but we do not consider prospective CSLI in this case. See note 24, supra.

[37] Both 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 -- this is not an appropriate case in which to establish 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. Nevertheless, it would be reasonable to assume that a request for historical CSLI of the type at issue in this case 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.

465 Mass. at 382 (no need to decide dimensions of individual's expectation "not to be subjected to extended GPS electronic surveillance by the government, targeted at his movements," because police GPS vehicle tracking for thirty-one days was sufficient to trigger defendant's reasonable expectation of privacy).

In the present case, the defendant made a showing of a subjective privacy interest in his location information reflected in the CSLI records,[38] and for all the reasons we have considered here, we conclude that this interest is one that our society is prepared to recognize as reasonable. See Katz, 389 U.S. at 361 (Harlan, J., concurring); Montanez, 410 Mass. at 301. Accordingly, the government-compelled production of the defendant's CSLI records by Sprint constituted a search in the constitutional sense to which the warrant requirement of art. 14 applied.

c. The exclusionary rule. Finally, the Commonwealth contends that even if the defendant had a reasonable expectation of privacy in the CSLI, the exclusionary rule should not apply because there was no government misconduct, the governing law was unclear, and excluding evidence of the CSLI in this instance can

---

[38] In support of his motion to suppress, the defendant submitted an affidavit stating that he acquired his cellular telephone for his own personal use, never permitting the police or other law enforcement officials access to his telephone records. The Commonwealth makes no argument that the affidavit fails to support a subjective privacy interest on the defendant's part.

have no real deterrent effect.

The Commonwealth obtained the CSLI in 2004 pursuant to a § 2703(d) order that the Commonwealth properly sought and obtained from a Superior Court judge, and no one disputes that the order met the "specific and articulable facts" standard of that statute. At the time, there was no decision by the Supreme Court or, it appears, any lower Federal court suggesting that notwithstanding the government's compliance with the requirements of 18 U.S.C. § 2703(c)(1)(B) and (d), under the Fourth Amendment, a search warrant based on probable cause was required. Nor was there a Massachusetts decision suggesting that art. 14 required a warrant. While the Commonwealth has argued consistently in this case that compliance with § 2703 is all that is necessary, it also has suggested -- before the motion judge and in this court -- that Trooper McCauley's affidavit submitted in support of the Commonwealth's application for a § 2703(d) order demonstrated the requisite probable cause -- i.e., probable cause to believe "that a particularly described offense has been, is being, or is about to be committed, and that [the CSLI being sought] will produce evidence of such offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit such offense." See Connolly, 454 Mass. at 825. In light of the particular circumstances of this case described in the previous paragraph, we conclude that it is appropriate to vacate the allowance of the defendant's motion to suppress in order to permit the motion

judge (or another Superior Court judge) on remand to consider whether the Commonwealth's 2004 application for the § 2703(d) order met the requisite probable cause standard of art. 14. If the judge concludes that the probable cause standard is met, the defendant's motion to suppress should be denied, and if not, the motion should be allowed.

d. Effect of this opinion. Finally, we consider whether this opinion announces a new rule of law and, if so, the scope of its retroactive application. See Commonwealth v. Sylvain, 466 Mass. 422, 428 (2013) ("the determination whether a case announces a 'new' rule is at the heart of the retroactivity analysis"). Adopting the United States Supreme Court's analysis set out in Teague v. Lane, 489 U.S. 288, 301 (1989), this court has long defined a new rule as one in which "the result was not dictated by precedent existing at the time the defendant's conviction became final." Commonwealth v. Bray, 407 Mass. 296, 301 (1990), quoting Teague, supra. "Under the Teague-Bray framework . . . [i]f a rule is 'new,' it applies only to defendants whose cases are not final unless two narrow exceptions apply;[39] if a rule is 'old,' it also applies retroactively to

---

[39] The two exceptions to prospective application of a new rule under Teague v. Lane, 489 U.S. 288, 311-313 (1989), and Commonwealth v. Bray, 407 Mass. 296, 300 (1990), are when a rule is "substantive," defining a class of conduct that cannot be deemed criminal, or prohibiting imposition of a type of punishment on a particular class of defendants; and when the rule establishes a "watershed" rule of criminal procedure that is "implicit in the concept of ordered liberty," implicating the fundamental fairness of the proceeding. See Diatchenko v. District Attorney for the Suffolk Dist., 466 Mass. 655, 665

defendants whose cases were final at the time the rule was announced." Sylvain, 466 Mass. at 433 (footnote and citation omitted). See Diatchenko v. District Attorney for the Suffolk Dist., 466 Mass. 655, 664-667 (2013).

Here, as just discussed, neither the statute, 18 U.S.C. § 2703(d), nor our cases, have previously suggested that police must obtain a search warrant in addition to a § 2703(d) order before obtaining an individual's CSLI from his or her cellular service provider. See Earls, 214 N.J. at 589 ("Although the parties dispute what might have been gleaned from earlier decisions, neither our case law nor the statute required a warrant for [cellular telephone] location information"). In holding here that the Commonwealth generally must obtain a warrant before acquiring a person's historical CSLI records, this opinion clearly announces a new rule. See id.

That being the case, and in accordance with the Teague-Bray framework, this new rule applies only to cases in which a defendant's conviction is not final, that is, to cases pending on direct review in which the issue concerning the warrant requirement was raised.[40] See Commonwealth v. Figueroa, 413

(2013), quoting Teague, supra at 311; Commonwealth v. Sylvain, 466 Mass. 422, 428 n.6 (2013).

[40] In part 4.c of this opinion, we determined that the Commonwealth should have an opportunity on remand to show that its application for the § 2703(d) order satisfied the probable cause standard of art. 14. In cases pending on direct review where the issue of the warrant requirement was raised, the Commonwealth may seek a similar opportunity.

Mass. 193, 202-203 (1992), S.C., 422 Mass. 72 (1996), quoting Commonwealth v. Libran, 405 Mass. 634, 645 (1989), and cases cited.[41] Cf. Galliastro v. Mortgage Elec. Registration Sys., Inc., ante , (2014) (applying similar rule in civil case). The warrant requirement we announce in the present case will not

---

[41] In Commonwealth v. Figueroa, 413 Mass. 193, 202-203 (1992), S.C., 422 Mass. 72 (1996), citing Bray, 407 Mass. at 298-299 (among other cases), this court applied to the defendant the rule that it had recently announced in Commonwealth v. Stockhammer, 409 Mass. 867 (1991), concerning a defendant's access to a complainant's treatment records in sexual assault cases -- a rule held to be based on art. 12 of the Massachusetts Declaration of Rights, see id. at 884 -- because Figueroa's case was on direct appeal when Stockhammer was decided, and he had preserved the issue at trial. We observed in Figueroa that if a newly announced criminal rule is not applied to other defendants who had raised the same issue and whose convictions were not final, it would "violate[] the principle of treating similarly situated defendants the same." Figueroa, supra at 202, quoting Bray, supra at 299, quoting Griffith v. Kentucky, 479 U.S. 314, 323 (1987).

In Griffith, 479 U.S. at 328, the Supreme Court held that a "new" rule for the conduct of criminal prosecutions applies to the case announcing the rule and cases in which the defendants' convictions are not final. Soon thereafter, this court interpreted the Griffith case as applying only to new rules based on the Federal Constitution, and as not binding on this court where a new rule was based on a State law source. See Commonwealth v. Waters, 400 Mass. 1006, 1007 (1987). See also Commonwealth v. Bowler, 407 Mass. 304, 306 (1990). Cf. Commonwealth v. D'Agostino, 421 Mass. 281, 284 n.3 (1995). We do not have reason here to question the interpretation of the Griffith decision's reach in Waters, supra, but subsequent to Waters, in applying the Teague-Bray framework in cases analyzing the scope of a new criminal rule based on the Massachusetts Declaration of Rights, this court has consistently referenced with implicit approval the principle that a new criminal rule applies to "those cases still pending on direct review." See Diatchenko, 466 Mass. at 664; Sylvain, 466 Mass. at 433, 436; Figueroa, 413 Mass. at 202-203. See also Bray, 407 Mass. at 300-301.

apply retroactively to cases on collateral review.[42]

5. Conclusion. For the reasons discussed, the order allowing the defendant's motion to suppress is vacated, and the case is remanded to the Superior Court for further proceedings consistent with this opinion.

So ordered.

---

[42] The rule announced in this case, that the Commonwealth must generally obtain a search warrant in order to obtain a person's CSLI records from a cellular service provider, is clearly not "substantive" or a rule that implicates procedures "implicit in the concept of ordered liberty." Diatchenko, 466 Mass. at 665, quoting Teague, 489 U.S. at 311. Accordingly, neither of the two narrow exceptions to prospective application of a new rule applies.

GANTS, J. (dissenting, with whom Cordy, J., joins). There are at least two different types of historical cell site location information (CSLI). Telephone call CSLI (the type sought by the Commonwealth and ordered by the court in this case) provides the approximate physical location (location points) of a cellular telephone only when a telephone call is made or received by that telephone. Registration CSLI (the type not sought by the Commonwealth or ordered by the court, and therefore the type not at issue in this case) provides the approximate physical location of a cellular telephone every seven seconds unless the telephone is "powered off," regardless whether any telephone call is made to or from the telephone. Telephone call CSLI is episodic; the frequency of the location points depends on the frequency and duration of the telephone calls to and from the telephone. Registration CSLI, for all practical purposes, is continuous, and therefore is comparable to monitoring the past whereabouts of the telephone user through a global positioning system (GPS) tracking device on the telephone, although it provides less precision than a GPS device regarding the telephone's location. The court recognizes the differences between telephone call CSLI and registration CSLI, and then conducts its analysis under art. 14 of the Massachusetts Declaration of Rights as if those differences have no constitutional consequence or as if the court ordered the production of registration CSLI. I believe that those differences have fundamental constitutional consequence with respect to both the reasonableness of the expectation of

privacy under the third-party doctrine and the extent of the intrusion on privacy, and therefore I respectfully dissent.

In Smith v. Maryland, 442 U.S. 735, 743 (1979), the United States Supreme Court held, under what has become known as the third-party doctrine, that telephone users had no subjective expectation of privacy in the telephone numbers they dialed because they "typically know that they must convey [the telephone numbers they call] to the [tele]phone company; that the [tele]phone company has facilities for recording this information; and that the [tele]phone company does in fact record this information for a variety of legitimate business purposes." The Court also declared that, even if the defendant "did harbor some subjective expectation that the [tele]phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."'" Id., quoting Katz v. United States, 389 U.S. 347, 361 (1967). The Court noted that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, supra at 743-744, citing United States v. Miller, 425 U.S. 435, 442 (1976) (bank depositor has no legitimate expectation of privacy in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business"). See, e.g., Couch v. United States, 409 U.S. 322, 335-336 (1973) (individual may not invoke privilege against self-incrimination under Fifth Amendment to United States Constitution to protect financial and

tax records held by his accountant); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion) (government agents did not violate Fourth Amendment to United States Constitution by listening to conversations between defendant and cooperating witness that they heard because witness secretly wore transmitter); Hoffa v. United States, 385 U.S. 293, 302 (1966) (Fourth Amendment does not protect "wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"); Lopez v. United States, 373 U.S. 427, 437-438 (1963) (same, applied to secret consensual recording of attempted bribe to Internal Revenue Service agent). In each of these cases, the Supreme Court held that an individual enjoys no constitutional protection from the government obtaining information that he voluntarily furnished to a third party to advance the individual's interest, whether that purpose is to make a telephone call, engage in banking transactions, prepare tax forms, confess wrongdoing, or attempt to pay a bribe.

In the instant case, the court acknowledges that we have "applied in substance the Supreme Court's third-party doctrine" but have also recognized that art. 14 may, under certain circumstances, provide more substantive protection than is provided under the third-party doctrine. Ante at , citing Commonwealth v. Blood, 400 Mass. 61, 68 n.9 (1987), and Commonwealth v. Buccella, 434 Mass. 473, 484 n.9 (2001), cert. denied, 534 U.S. 1079 (2002). The court declares that "we see no reason to change our view that the third-party doctrine applies

to traditional telephone records," but concludes that "the distinctive characteristics of cellular telephone technology and CSLI" require the conclusion that, under art. 14, the third-party doctrine should not be applied to CSLI. Ante at .

The "distinctive characteristics" that the court identifies that lead to this conclusion, however, are characteristics of registration CSLI, not the telephone CSLI that the Commonwealth sought in this case and that the court ordered to be produced. Because nearly everyone now carries a cellular telephone and because CSLI "tracks the location of a cellular telephone user," the court claims that "[i]t is evident that CSLI implicates the same nature of privacy concerns as a GPS tracking device," and is arguably even more intrusive of privacy because it tracks the location of the cellular telephone carried on the person of its user rather than the location of his or her vehicle. Ante at , , . The court essentially contends that cellular telephone users are speaking on their cellular telephone so often that telephone CSLI will provide nearly as many location points as a GPS tracking device or registration CSLI, so that telephone CSLI is analogous to a GPS device in a cellular telephone user's pocket. The court rests this contention on its own experience ("As anyone knows who has walked down the street or taken public transportation in a city like Boston, many if not most of one's fellow pedestrians or travelers are constantly using their cellular telephones as they walk or ride," see ante at) and on data regarding the annual volume of voice minutes used on

cellular telephones in the United States ("In 2012, there were 2.3 trillion voice minutes of use on wireless devices such as cellular telephones in the United States," see ante at note 29).

But this contention is empirically incorrect. According to the Wireless Association, the same source the court relies on for the annual number of voice minutes, there are more cellular telephones in the United States than United States residents.[1] Therefore, the total United States population conservatively estimates the number of cellular telephones in active operation in the United States. If we take the annual volume of voice minutes (2.3 trillion), and divide it by the multiple of the total United States population in July, 2012 (313.87 million), and the number of minutes in a year (525,600), we learn that cellular telephone users spoke on the telephone in 2012 only 1.4 per cent of the day (0.01394). See CTIA: The Wireless Association, Wireless Quick Facts (Nov. 2013), http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts (last viewed Feb. 14, 2014); United States Census Bureau, Annual Estimates of Resident Population: 2013 Population Estimates (Dec. 2013), http://factfinder2.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk (last viewed Feb. 14, 2014). This rough

---

[1] "Wireless penetration," defined as "[the number] of active units divided by the total [United States] and territorial population," in December, 2012, was 102.2 per cent. CTIA: The Wireless Association, Wireless Quick Facts (Nov. 2013), http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts (last viewed Feb. 14, 2014).

estimate is corroborated by a survey conducted by PriceWaterhouseCoopers, which found that the average cellular telephone subscriber is speaking on the telephone 673 minutes per month, or 1.5 per cent of the day (0.01536). PriceWaterhouseCoopers, Real Time: The Growing Demand for Data, 2012 North American Wireless Industry Survey 36 (Apr. 2013), http://www.pwc.com/en_US/us/industry/communications/publications/assets/pwc-north-american-wireless-industy-survey-2012.pdf (last viewed Feb. 14, 2014). Therefore, while it may seem as if Americans are always talking on their cellular telephones, they are actually doing so less than two per cent of the day. Therefore, there is a world of difference between telephone CSLI and registration CSLI in terms of the location points they will reveal and the degree to which they will intrude on personal privacy.

The telephone CSLI obtained in this case is much closer to the "traditional telephone records" that, the court agrees, are still governed by the third-party doctrine. While we have long accepted that the Commonwealth may obtain cellular telephone toll records without a search warrant supported by probable cause, it bears noting that the information revealed by those records intrudes deeply on personal privacy. Just as registration CSLI can "provide an intimate picture of one's daily life," by revealing "the people and groups they choose to affiliate with and when they actually do so," ante at , quoting State v. Earls, 214 N.J. 564, 586 (2013), so, too, can telephone toll

records, which can be used to identify who one speaks with on the telephone and how often.

Before cellular telephones, when telephones were located only in one's home or business, traditional telephone records effectively revealed the location of the telephone user at the time of the call; if a person made a telephone call from a home telephone, the person was at home.[2] Therefore, location information is not unique to telephone call CSLI; what has changed is the mobility of the telephone. I recognize that, because of the mobility of a cellular telephone, telephone call CSLI will provide many location points outside a user's home or place of business, and these location points may provide a patchwork that will intrude on the user's privacy to the extent that they reveal where the user is located when making or receiving calls on the telephone. But this patchwork of location points, while intrusive of privacy, is less intrusive than the patchwork of personal affiliations that can be learned from traditional telephone toll records. I also recognize that the degree of intrusion on privacy will depend on the number of calls the user makes and receives. But this is also true about traditional telephone records; the more telephone calls a person makes and receives, the more will be revealed regarding the

---

[2] Of course, just as with cellular telephones, the owner of the telephone line may not be the person using the telephone, or it may be used by multiple persons. The only difference between the traditional home telephone and a cellular telephone is that the latter is more likely to have a single user.

persons the individual speaks with and the frequency of those calls.

Telephone CSLI, like telephone toll records, also fits within the traditional justification for the third-party doctrine. Every person who uses a cellular telephone recognizes that the location of the telephone matters in determining whether there is cellular service and, where there is service, in determining the quality of the telephone connection, which is why at least one cellular telephone company advertises "more bars in more places." Therefore, every person who uses a cellular telephone recognizes, at least implicitly, that a cellular telephone company must identify the location of a cellular telephone, as well as the telephone number called, before a call can be successfully made from a cellular telephone. Therefore, while a cellular telephone user may not know that the telephone company records and keeps this information, or want it kept, the user should know that location information, as well as the telephone number, must be provided to the telephone company whenever he makes or receives a telephone call. See In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013) (information, such as telephone user's location, that cellular telephone company needs to route telephone communications "appropriately and efficiently" falls within third-party doctrine).

I agree with the court and Justice Sotomayor that, in this digital age "it may be necessary to reconsider the premise that

an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Ante at note 35, quoting United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). In the context of cellular telephone records, I would not extend the third-party doctrine to include information that is not necessary to the successful completion of a telephone call, and therefore would not apply the third-party doctrine to registration CSLI. A person obtains a cellular telephone for the purpose of making and receiving telephone calls, not to permit the telephone company or another third party to track the user's location when the person is not using the telephone. Telephone CSLI is obtained by the telephone company to advance the telephone user's interest in making or receiving telephone calls and is necessary to the successful completion of those telephone calls, while registration CSLI is not necessary because a telephone call may successfully be made even if the telephone had been powered off moments before.[3] Where telephone toll records are covered by the third-party

---

[3] The court, quoting State v. Earls, 214 N.J. 564, 587 (2013), declares: "People buy [cellular telephones] to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a [cellular telephone] to share detailed information about their whereabouts with the police." Ante at . It is true that no one buys a cellular telephone "to share detailed information about their whereabouts with the police," but it is also true that no one buys a cellular telephone to share with the police the telephone numbers of the calls they are dialing and receiving. In terms of the third-party doctrine, the meaningful distinction between telephone cell site location information (CSLI) and registration CSLI is not the cellular telephone owner's willingness to share private information with the police.

doctrine, and where location information is as necessary as the telephone number itself to the successful completion of a telephone call, I cannot find any principled reason why this doctrine would not also apply to telephone call CSLI.[4] The court claims that there is a "significant difference" between cellular telephone toll records and CSLI in that "[n]o cellular telephone user . . . voluntarily conveys CSLI to his or her cellular service provider in the sense that he or she first identifies a discrete item of information or data point like a telephone number . . . and then transmits it to the provider." Ante at . The difference is less than the court claims. First, it has been many years since a telephone caller had to make a call by dialing the operator at the telephone company, providing the operator with the number to be called, and asking the operator to connect you with that number. Today, a telephone caller no more voluntarily conveys a number to the telephone company than he voluntarily conveys his location to the telephone company, but he implicitly knows that the telephone company's computers need to know both for the call to be successfully connected. Second, for incoming telephone calls, the person receiving the call does not dial any number or otherwise convey any number, but the telephone number of the caller is nonetheless included in the cellular telephone toll records. Telephone CSLI is certainly different

---

[4] I offer no opinion as to whether the third-party doctrine should apply to CSLI obtained when a cellular "smartphone" is using the Internet.

from telephone toll records, and provides different private information, but if the principle justifying the third-party doctrine for telephone toll records is that the information is necessary to the successful completion of telephone calls, there is no principled reason why the third-party doctrine should apply to telephone toll records but not to telephone call CSLI.[5]

Separate and apart from the third-party doctrine, the court's analogy of CSLI to GPS tracking devices affixed to automobiles also is far weaker with telephone call CSLI than with registration CSLI. As I have noted, GPS tracking is continuous; registration CSLI is nearly so, providing location points for the cellular telephone every seven seconds. Telephone call CSLI is episodic, not continuous, and therefore its location points are not a continuous or continual line, but simply a patchwork of points. The extent to which that patchwork can reveal an intelligible picture of where the user goes and whom the user visits, and therefore the degree of intrusion on privacy, will depend both on the frequency of telephone calls and the duration of the CSLI request. We concluded in Commonwealth v. Rousseau,

---

[5] The court contends that there is the "probability that, as CSLI becomes more precise, cellular telephone users will be tracked in constitutionally protected areas," namely one's home. Ante at . The court noted, however, that the GPS "type of location tracking is not at issue here," ante at note 21, and there is nothing in the record to suggest that CSLI is likely to become so precise in the immediate future that it will identify where inside a home a person is located. The theoretical possibility that telephone call CSLI may enable the police in the future to track a person's movement within the home is not an independent ground to require a search warrant supported by probable cause.

465 Mass. 372, 382 (2013), "that under art. 14, a person may reasonably expect not to be subjected to extended GPS electronic surveillance by the government, targeted at his movements, without judicial oversight and a showing of probable cause." We did not decide "how broadly such an expectation might reach and to what extent it may be protected," or what duration less than thirty days would suffice as "extended" GPS electronic surveillance. Id.

Where that durational line is drawn, that is, determining when a locational surveillance (whether through GPS or CSLI) becomes so intrusive as to constitute an invasion of the reasonable expectation of privacy, is critical in finding the appropriate balance between personal liberty and legitimate law enforcement interests. No CSLI, whether it be telephone CSLI or registration CSLI, may be obtained by the Commonwealth without obtaining judicial authorization under 18 U.S.C. § 2703(d) (2006), and such authorization requires a showing of "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." This may be "essentially a reasonable suspicion standard," In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 707 F.3d 283, 287 (4th Cir. 2013), but it is merely reasonable suspicion that the CSLI records "are relevant and material to an ongoing investigation," not reasonable suspicion

that the user of the telephone has committed, is committing, or is about to commit an offense. Therefore, where the police receive informant information of uncertain reliability that a particular gang was involved in a shooting, the police under this standard may follow up on that lead by gathering the CSLI records at or around the time of the shooting for each gang member to determine whether they were in the vicinity of the shooting, even if they have nothing more to suggest that any particular gang member participated in the shooting.

Where a search warrant is required, however, the standard becomes "probable cause to believe 'that a particularly described offense has been, is being, or is about to be committed, and that [the CSLI being sought] will produce evidence of such offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit such offense.'" Ante at , quoting Commonwealth v. Connolly, 454 Mass. 808, 825 (2009). Because of the probable cause requirement and, more importantly, because there must be probable cause that the CSLI will produce evidence implicating the telephone user in a crime, the police will not be able to obtain a search warrant unless they already have obtained significant other information implicating the telephone user in a crime. Therefore, if a search warrant were required for all CSLI, regardless of duration, the police would not be able to use CSLI in my hypothetical shooting case to identify or eliminate possible suspects. A search warrant may appropriately be

required where the CSLI, because of its duration and the number of location points it will identify, will reveal so much about the private life and personal affiliations of the telephone user as to invade the reasonable expectation of privacy, but it is not appropriate where the duration will reveal only where the telephone user was at a particular time or over a brief period of time. And, if the search warrant requirement is given inappropriate breadth, it will significantly diminish the ability of law enforcement to solve and to prove crimes, which so often depends on proving the whereabouts of a suspect at the time of the crime through his or her cellular telephone location.[6]

Because the court treats the telephone CSLI at issue in this case as if it were registration CSLI, and fails to recognize that this distinction is critical to the applicability of the third-party doctrine, to the adaptation of our GPS tracking jurisprudence, and to the determination whether the duration of

---

[6] The court appears to recognize this concern where it declares that "it would be reasonable to assume that a request for historical CSLI of the type at issue in this case 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." Ante at note 37. However, because the court characterized this as a reasonable assumption rather than a safe harbor rule, and prefaced it with the declaration that "this is not an appropriate case in which to establish 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," prosecutors who procure CSLI for six hours or less through a § 2703(d) order without also obtaining a search warrant still risk the suppression of this CSLI evidence. The court need not in this case "establish a temporal line of demarcation," but it should have established a safe harbor well within that "temporal line" to protect the invaluable investigative use of short-term CSLI.

CSLI surveillance invades the reasonable expectation of privacy, I respectfully dissent. Because the court order in this case allowed only for production of telephone CSLI over a two-week period, not registration CSLI, I would conclude under the third-party doctrine that the defendant had no reasonable expectation of privacy in his location points when he was making or receiving telephone calls, and reverse the judge's allowance of the motion to suppress.