TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Treatises

ISSUES PRESENTED

I. Whether the motion judge erred in taking judicial notice of facts that were material to the motion to suppress but which cannot be said to be indisputably true.

II. Whether the motion judge erred in suppressing cell tower records where there was no government action and where the defendant failed to demonstrate a reasonable expectation of privacy in his cell phone records or in the location which they revealed.

III. Whether the exclusionary rule should apply where the records were obtained through a court order and there was no police misconduct.

STATEMENT OF THE CASE

On July 29, 2011, a Suffolk County grand jury indicted the defendant, Shabazz Augustine, for the murder of Julaine Jules, in violation of G.L. c. 265, § 1 (CA.3).[1]

On November 15, 2012, the defendant filed a motion to suppress Cell Site Location Information "(CSLI)," arguing that this information was obtained pursuant to a warrantless search and seizure in violation of the Fourth, Fifth, Sixth, and Fourteenth

[1] "(CA._)" herein refers to the Commonwealth's record appendix while "(Tr._:_)" refers to the two volumes of transcript from the motion to suppress hearings.

Amendments to the United States Constitution and Articles 12 and 14 of the Massachusetts Declaration of Rights (CA.5; 9-42). After two non-evidentiary hearings on January 16, 2013 and February 15, 2013 (CA.6),[2] Judge Janet L. Sanders allowed the defendant's motion on February 26, 2013, noting that a written memorandum was to follow (CA.6). On February 28, 2013, the Commonwealth filed notice of appeal (CA.6; 112-113).

On March 4, 2013, the Commonwealth filed an application for interlocutory review (CA.127-147). On April 2, 2013, Judge Sanders issued a "Memorandum of Decision and Order" on the defendant's motion to suppress (CA.114-126). After receiving this decision, the Commonwealth filed a supplemental application for interlocutory review on April 23, 2013 (CA.157-170). On May 2, 2013, the Single Justice Gants, J., allowed the Commonwealth's application and ordered that it be heard by the Full Bench (CA.171).

---

[2] During the January 16 hearing the judge took evidence related to a motion to suppress statements not at issue here (CA.6). She also heard a preliminary argument as to the motion to suppress CSLI (CA.6; Tr. 1:67-92).

STATEMENT OF FACTS

1. The Commonwealth's Case.

On August 24, 2004, Julaine Jules left her work place in South Boston at approximately 7:00 pm and was not seen again until her body was discovered in the Charles River on September 19, 2004 (CA.12; 43). Because her body was discovered in a section of the Charles River that fell within the boundary of Middlesex County, the investigation into Jules's disappearance and death commenced there (Tr.1:80). During this investigation, on September 22, 2004, the Middlesex County District Attorney's Office sought and obtained a judicial order pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act seeking CSLI maintained by Sprint for the defendant's cellular phone number (617) 905-7830 (CA.43; Tr. 1:80).

Under the Stored Communications Act, the government can require the provider of an electronic communication service to disclose "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)" by obtaining a judicial order pursuant to 18 U.S.C. § 2703(d). *See* 18 U.S.C. § 2703(c)(1). To obtain an order pursuant to § 2703(d), the government must demonstrate to a court "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." 18 U.S.C. § 2703(d). Under the provisions of § 2703(d), the government is not required to obtain a search warrant for such information. The order here granted access to historic CSLI from August 24, 2004 through September 7, 2004 (CA.19).

In late 2007 or early 2008, the investigation into Jules's death was turned over to the Suffolk County District Attorney's Office after evidence suggested that the incidents related to Jules's disappearance and death took place in Suffolk County (Tr.1:80). The Suffolk County District Attorney's Office commenced a Grand Jury investigation, which culminated in 2011 with an indictment charging defendant with first degree murder (CA.3).

2. The Motion To Suppress.

During the first hearing on the defendant's motion to suppress CSLI, the defendant asked the judge to take judicial notice of how a cell phone technically works (Tr.1:73). The Commonwealth reserved the right to object (Tr.1:74), and the judge indicated that she did not think there was any dispute

"as to how cell phone technology works with regard to these locations" (Tr.1:74).

At the second hearing, the Commonwealth argued that CSLI provided a very limited type of information, (Tr.2:17, 22-25, 28-29), which did not reveal a precise location (Tr.24). The Commonwealth contested that CSLI revealed a precise location, explaining to the judge that CSLI can only show that an individual cell phone pinged off a particular public tower in Malden, which could be used to demonstrate that he was in Malden and not in Boston (Tr.2:24). The Commonwealth also argued that it was the defendant's burden to show that the CSLI was more discerning in this case, (Tr.2:23; 25), which he could do by demonstrating how "densely the cell towers [were] located throughout the city" (Tr.2:25). The Commonwealth argued throughout the hearing that the defendant simply had not shown that he had any expectation of privacy in this type of information (Tr.2:18, 20-21, 23, 25-26).

During this hearing, the parties also discussed whether CSLI was like GPS in terms of the how precise a location it revealed. The judge recognized that she had no basis to find that CSLI "can define location with the precision of GPS" (Tr.2:28). In response,

defense counsel stated that he "was not going to say [CSLI is] the same as GPS" (Tr.2:29). The Commonwealth reiterated that it did not believe CSLI was in any way analogous to GPS (Tr.2:33).

3. The Memorandum of Decision and Order of the Motion to Suppress.

The motion judge began her memorandum of decision by explaining, "[b]ecause there was no dispute as to the relevant facts," she "did not hold an evidentiary hearing" (CA.115). Nevertheless, the motion judge explained that "some factual context as to the technology at issue" was needed (CA.115). She noted that because "[t]he parties agreed that this Court could take 'judicial notice' of facts related to this technology" (CA.115), she would make findings as to how a cell phone worked (CA.115). She found that

> unlike conventional land lines phones, cellular phones use radio waves that connect the user's handset to the telephone network. These radio waves are picked up by a system of "cell sites" or base stations spread throughout the geographical coverage area. These sites include a cell tower, radio transceiver and base station controller. Radio waves are transmitted to this base station any time a cell phone user makes or receives a call or text message. In addition, through a process called "registration," a cell phone will periodically identify itself to a cell tower whenever a phone is on, whether a call is made or not.

(CA.115).

The judge then made findings as to how location is revealed using cell towers (CA.115). She found

> By correlating the precise time and angle at which a phone's signal arrives at different cell towers, one can determine a cell phone's location. It is this Cell Site Location Information (CSLI) that is at issue here. The cell phone provider collects and stores historical CSLI for network management and marketing. The cost of collecting this data has declined, with a trend toward more extensive archiving of this information.
>
> Cell towers were initially placed far apart so as to maximize coverage. Nowadays with cell phones in common use, the number of towers has increased dramatically, tripling in the last decade. The result is that a cell phone user's location can be pinpointed with much more exactitude, thus diminishing the difference between CSLI and the Global Positioning System, or GPS.

(CA.115-116).

The judge ruled that obtaining CSLI without a warrant violated art. 14 of the Massachusetts Declaration of Rights because CSLI is like GPS in that it revealed a precise location (CA.116, 122-123). She explained that in order to take the Commonwealth's argument that "CSLI is far less precise in determining an individual's location than" GPS seriously, "this Court would have to close its eyes to reality: as cell phones have become ubiquitous, cell towers too have

proliferated and, through a process of 'triangulation' among towers, CSLI is now no less accurate than GPS in pinpointing location (except perhaps in remote rural areas)" (CA.122-123).

The judge was also not persuaded that because CLSI involved access to historic data for a limited period of time it was different than the real time monitoring of an individual through GPS as considered by the Supreme Court in *United States v. Jones*, 132 S.Ct. 945 (2012) (CA.123). She held that "[t]he temporal difference between prospective and historic location tracking has no bearing on whether one has any reasonable expectation of privacy in that information" (CA.124). "A more satisfactory answer," she explained,

> is that the duration of the monitoring is irrelevant. The fact is that technology has made it possible for law enforcement to access information which it would have never been able to obtain by standard police surveillance techniques. This is particularly true where the CSLI is historical since it allows the government to do what has hitherto been impossible and literally reconstruct a person's movements in the past. Where there is probable cause to believe that the person has committed a crime, allowing the government to access this information is clearly a good thing. However, without that minimal limit on government power, all of us (at least those of us with cell phones) are at risk.

(CA.125).

The judge also rejected the Commonwealth's argument that the defendant did not have any expectation of privacy in CSLI because he voluntarily transmitted this information to a third party, his cell phone provider (CA.123-124). She ruled that while "[t]he ordinary cell phone user may understand that radio waves are sent out to connect his calls" it "requires a jump in logic to conclude that the user is also aware that his provider is making a record of the location from which he made the call and is storing it for some indefinite period" (CA.124). "More significant," the judge held, "there is no overt or affirmative act by the user whereby she voluntarily exposes her location to a third party: CSLI is generated automatically without the cell phone user's participation beyond the act of making a call" (CA.124). "Finally," she explained, "CSLI can be generated even without a call being made since, through a process of 'registration,' a cell phone will periodically identify itself to a cell tower whenever a phone is on, whether a call is made or not" (CA.124); and "[i]n short, this Court fails to see how one 'assumes the risk' that the government will be

able to track one's movements simply by carrying a cell phone on one's person" (CA.124).

SUMMARY OF THE ARGUMENT

I. The judge erred when she took "judicial notice" of facts related to the precision of location revealed by CSLI. First, because the parties never agreed to those facts or agreed that she could take judicial notice of such facts. Second, because they were not the type of indisputably true facts a judge could properly take judicial notice of. Compounding this error, the actual CSLI record itself that was provided in response to the 2703(d) order was never marked as an exhibit or submitted in support of the defendant's motion. Thus, the judge had no basis to find that the CSLI in this instance revealed any location let alone as precise a location as GPS and relieved the defendant of his burden to demonstrate that he had a constitutionally protected interest in this information (pp. 11-27).

II. The judge erred in finding that a search in the constitutional sense occurred. First, because there was no governmental action as the surveillance was not conducted at the direction or with the involvement of the government. Second, because CSLI is a business record held by a third party that the defendant failed

to demonstrate he had an expectation of privacy in. Third, because the defendant failed to manifest an expectation of privacy in the location revealed in CSLI or in not being so surveilled (pp. 27-53).

III. The judge erred in ruling that the exclusionary rule should apply because the records were obtained through a court order with a supporting affidavit that established probable cause and there was no police misconduct (pp. 53-58).

ARGUMENT

I. THE JUDGE ERRED IN TAKING JUDICIAL NOTICE OF FACTS RELATED TO THE PRECISION OF THE LOCATION REVEALED BY CSLI.

The judge improperly took judicial notice of a number of facts. "A judge's reliance on information that is not part of the record implicates fundamental fairness concerns." *Commonwealth v. O'Brien*, 423 Mass. 841, 848 (1996) (citing *White v. White*, 40 Mass. App. Ct. 132, 141-142 (1996)). For that reason, judicial notice "cannot be taken of material factual issues that can only be decided by the fact finder on competent evidence." *Commonwealth v. Kirk*, 39 Mass. App. Ct. 225, 229 (1995). "Matters are judicially noticed only when they are indisputably true." *Nantucket v. Beinecke*, 379 Mass. 345, 352 (1979); *accord O'Brien*, 423 Mass. at 848. "A judicially

noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to resources whose accuracy cannot reasonably be questioned." Mass. G. Evid. § 201(b) (2012).

Here, the judge stated that the parties agreed that the court could take "judicial notice" of facts related to cell phone technology (CA.115). She then went on to use what she characterized as judicially-noticed facts to make findings about how a cell phone works, how cell site data can reveal an individual's location, and how precise of a location the data reveals (CA.115). However, the Commonwealth never agreed that the judge could take judicial notice of all of those facts. At the first hearing, the Commonwealth reserved the right to object to the judge taking judicial notice of this type of information (Tr.1:74). In its memorandum in opposition to the defendant's motion to suppress, the Commonwealth broadly defined how a cell phone works and what a cell site and cell site data is by relying on two cases: *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005) and *In re Application of the*

U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008) (CA. 44-45). To the extent that the Commonwealth agreed to stipulate to any facts, it was only general facts about how a cell phone works, what a cell site is, and that cell service providers maintain a record of CSLI as set forth in those two cases (*see* CA.44-45).

The Commonwealth never agreed to stipulate to any facts related to the precision of location revealed by CSLI. Compounding this error, the actual CSLI record itself that was provided in response to the 2703(d) order was never marked as an exhibit or submitted in support of the defendant's motion. Thus, the judge had no basis to find that the CSLI in this instance revealed any location let alone as precise a location as GPS. It is the defendant's burden to demonstrate that he had a constitutionally protected interest in this information, *see Commonwealth v. Montanez*, 410 Mass. 290, 301 (1991); *Commonwealth v. D'Onofrio*, 396 Mass. 711, 714-715 (1986), yet he failed to put that argument before the court at all. Indeed, defense counsel admitted at the motion hearing that he was not arguing that CSLI revealed as precise a location as GPS (Tr.2:29). Accordingly, the use of judicially

noticed facts improperly relieved the defendant of his burden. For this reason alone, the decision should be reversed.

The facts that the Commonwealth stipulated to outlined the basic facts about how a cell phone works and how a cell service provider normally keeps CSLI-type records (*see* CA.44-45). A cell phone is a radio that relies upon a network of cell sites to make and receive calls. *See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d at 750. A cell site is a geographical location containing a cell tower, radio transceiver, and base station controller. *Id*. The cell site sends and receives traffic from the cell phones that are near it to a switching office. *Id*. This switching office controls all the cell sites in the area. *Id*. at 751.

Cell phones and base stations communicate with each other on frequencies called channels. *Id*. When a cell phone is on it searches for the strongest channel provided by its service provider. *Id*. When it selects a channel, the cell phone sends a unique electronic serial number and mobile identification number to the cell site. *Id*. Most cell service providers maintain records of this information in

their ordinary course of business that identify – for any given cell phone number – the general location of the phone at a given time by the specific tower that transmitted the call and the specific "face" of the tower that served as the antenna. *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't*, 534 F. Supp. 2d at 590. The precision with which CSLI locates a certain cell phone depends on the proximity of the cell sites to each other in a given area. *See id*.

When the cell service provider records the cell site that carries the communication, it does not record the actual content of the communication itself. *See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. at 750. CSLI is maintained in large part for business purposes such as improving service and determining roaming charges based on the cell site that a subscriber's phone uses for a particular call. *See In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't*, 534 F. Supp. 2d at 590.

The background information above was appropriate for the judge to find because it was agreed to by both

parties. However, it was improper for the judge to take judicial notice of any other fact. Specifically, it was an error to make any finding about how precise a location CSLI revealed. At the second hearing, there was an active disagreement between the Commonwealth and the defendant as to how precise a location CSLI reveals. The Commonwealth argued that CSLI provided a very limited type of information, (Tr.2:17, 22-25, 28-29), which did not reveal a precise location (Tr.2:24). The defendant argued the opposite (Tr.2:10-16, 28-31). How precise a location is revealed by CSLI was a material issue to the motion, as indicated by the arguments made by both parties and by the judge's ultimate ruling that the motion should be allowed because CSLI revealed as precise a location as GPS (CA.122-123). Judicial notice cannot be taken of a material issue in dispute. *See Kirk*, 39 Mass. App. Ct. at 229. For that reason alone, the judge's order cannot stand.

That other courts have taken judicial notice of similar facts has no bearing on this issue. During the motion hearing, the defendant argued that the judge should take judicial notice of necessary facts because Judge David Lowy had done so in *Commonwealth v. Wyatt* No. ESCR2011-00693, 30 Mass. L. Rep. 270,

2012 Mass. Super. LEXIS 248 (Aug. 7, 2012) (Tr.1:76-77). In *Wyatt*, Judge Lowy took judicial notice of facts related to CSLI relying on *In re Application of the United States of America for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010),[3] to support his findings. In the S.D. Tex. case, which was recently reversed,[4] Judge Stephen Wm Smith, also took heard no evidence and elected instead to take judicial notice of facts related to CSLI based on a 2010 Congressional hearing. *Id*. A comparison of the facts as found by Judge Smith in the S.D. Tex. case to the materials related to the 2010 Congressional hearing demonstrate why judicial notice of these facts by Judge Smith in the S.D. Tex. case, Judge Lowy in *Wyatt*, and Judge Sanders here, was improper.

For example, in the S.D. Tex. case, the judge found

> New technology allows providers to locate not just the sector in which the phone is located, but also its position within the sector.

---

[3] Due to the length of this case name it is referred to hereinafter the "S.D. Tex. case."

[4] The Fifth Circuit recently reversed this decision in *In re: Application of the United States of America for Historical Cell Site Data*, 2013 U.S. App. LEXIS 15510 (July 30, 2013), holding that the defendant did not have a reasonable expectation of privacy in CSLI as it was a third party business record.

> By correlating the precise time and angle at which a phone's signal arrives at multiple sector base stations, a provider can pinpoint the phone's latitude and longitude to an accuracy within 50 meters or less. Emerging versions of the technology are even more precise.
>
> . . .
>
> Carriers typically create 'call detail record' that include the most accurate location information available to them.

In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 747 F. Supp. 2d at 833. The judge used the testimony of Professor Matt Blaze on June 24, 2010, at a congressional hearing on "ECPA Reform and the Evolution in Location Based Technologies and Services" to find those facts. From those findings, it appears that Blaze testified that each cell phone service provider has the ability to locate the precise location of a cell phone user within 50 meters and records that information in a call detail record. Looking at Blaze's testimony in context, however, shows that is not what he testified to.

While true that Blaze testified that new technology allows cell phone services providers to locate an individual's position within the sector and that certain products and upgrades can be used to "pinpoint a phone's location to an accuracy of 50

meters," he also explained that "these enhanced location technologies are not yet available in every network." ECPA Reform and the Revolution in Location Based Technologies and Services, Before the Subcomm. On the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 2, 27 (2010) (statement of Matt Blaze). He further stated that, "[w]hether locations are routinely tracked and recorded at times other than when calls are made or received depends on the policy of the particular carrier." 111th Cong. at 26 (statement of Blaze). While Blaze did testify that "carriers typically create 'call detail records' that include the most accurate location available to them," 111th Cong. at 27, he clarified that testimony in a follow-up letter to the Subcommittee, in which he explained, "[t]he degree of information that can be obtained from these records depends on the precise collection practices of the particular provider. Some providers may collect only information about the nearest tower." 111th Cong. at 135 (testimony of Blaze).

The problem with taking judicial notice of a small portion of Blaze's testimony is magnified when comparing it to other testimony from that same hearing. Another individual, Michael Amarosa, who

testified at that hearing, explained that CSLI "is an element of a carrier's network" that generally "presents the broad geographic area which can be used to identify the approximate region, quadrant or a more refined area of [a] call." 111th Cong. at 122 (questions for the record Michael Amarosa, Senior Vice President, TruePosition). "In most circumstances," he further explained, "the data is not precise enough to assist with identifying a location that can be used for an emergency dispatch." 111th Cong. at 122 (statement of Amarosa). Moreover, he testified that while his company provided technology that made it possible to locate a call within 150 feet, 111th Cong. at 95 (testimony of Amarosa), cell service providers do not use the technology unless the call has a certain trigger, such as if it is a call to 911. 111th Cong. at 96 (testimony of Amarosa). Indeed, Blaze agreed with that fact as he testified that cell service providers only locate a caller to that degree of accuracy when specifically asked to do so. 111th Cong. at 96 (testimony of Blaze). Cell service providers "do not collect these types of precise location information on consumer-level user in the ordinary course of business." Electronic Communications Privacy Act (ECPA), Part 2: Geolocation

Privacy and Surveillance, Before H. Subcomm. on Crime, Terrorism, Homeland Security and Investigations of the H. Comm. on the Judiciary, 113 Cong. 1, 7 (2013) (statement of Mark Eckenwiler, senior counsel Perkins Coie LLP).

It cannot be said then that there is agreement as to the precision that CSLI reveals a location at any given time. Blaze testified before Congress in both 2010 and again in April of 2013 that the precision of CSLI "will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less precise." 113 Cong. at 2 (statement of Blaze); 111th Cong. at 28-29 (statement of Blaze). In the same 2013 hearing, Mark Eckenwiler similarly testified that "[t]he degree to which CSLI reveals the location of a user's phone varies for several reasons" including how far apart the towers are spaced (which varies enormously), how heavily populated the area is, and how often the boundaries between the sectors of an individual cell tower change. 113 Cong. at 2 (statement of Eckenwiler). He further explained

> a particular communication is not always handled by the closest tower. Both natural terrain features (e.g., hills and valleys) and man-made structures interfere with line-of-sight radio transmission. Weather conditions, including precipitation or even humidity level, also may affect signal propagation.
>
> At times, the carrier antenna closest to the user's handset may even be entirely unavailable. This can result from local, temporary equipment or network outages, or simply from network congestion.

Id.

In sum, the Congressional testimony is that the type of location CSLI reveals is incredibly dynamic. It seems not to lend itself to generalization. While CSLI could in theory reveal a precise location, whether it actually does depends on a number of factors. The judge's findings here, however, do not reflect that this is the agreement about how precise a location CSLI will provide. For that reason, her judicially-noticed facts are not "indisputably true," should be set aside, and her order reversed. *See O'Brien*, 423 Mass. at 848; *Beinecke*, 379 Mass. at 352.

Additionally, the specific facts judicially noticed by the judge were not the type of facts that could be properly judicially noticed. The judge found that "a cell phone user's location can be pinpointed with much more exactitude, thus diminishing the

difference between CSLI and the Global Positioning System, or GPS" (CA.115-116). Such a fact -- that CSLI reveals a location akin to GPS -- was not supported by evidence or even argument at the hearing. The judge herself recognized that she had no basis to make such a finding (Tr.2:28).

Moreover, as demonstrated by both the 2010 and 2013 testimony of Blaze, whether CSLI reveals a precise location varies by customer, carrier, and day. 113 Cong. at 2 (statement of Blaze); 111th Cong. at 28-29 (statement of Blaze). Indeed, "[n]ot all location data is created or used equally. Mobile location data is derived from a variety of sources that have varying degrees of precision." Cy Smith, "FTC Staff Preliminary Report on Protecting Consumer Privacy" (Feb. 18, 2011), available at http://www.ftc.gov/os/comments/privacyreportframework/00438-58027.pdf (last visited 13 Aug. 2013). While GPS data may be very precise, "a cell site generated location can be up to a mile off." Smith, *supra,* at 3. Thus, the finding that CSLI reveals a location akin to that revealed by GPS is unfounded and cannot be said to be "indisputably true," *see O'Brien*, 423 Mass. at 848; *Beinecke*, 379 Mass. at 352, and should be set aside because it is clearly erroneous. *See*

Commonwealth v. Hilton, 450 Mass. 173, 178 (2007) ("A finding is clearly erroneous if it is not supported by the evidence, or when the reviewing court, on the entire evidence, is left with the firm conviction that a mistake has been committed."); *accord Commonwealth v. Antwan*, 450 Mass. 55, 61 (2007).

The judge also found that

> [c]ell towers were initially placed far apart so as to maximize coverage. Nowadays with cell phones in common use, the number of towers has increased dramatically, tripling in the last decade."

(CA.115). First, there is no citation to any source which shows where this fact is from. There is nothing to show where the number of towers has tripled in number whether it is the world, the United States, or Massachusetts. There was no evidence at the hearing that established how many cell towers are currently around greater Boston or how many cell towers were in the area in 2004 when the victim was killed. As such, there is no way to ascertain whether this fact is accurate or if it came from a source "who accuracy cannot be questioned" or whether this is a statistic that is subject to reasonable dispute. *See* Mass. G. Evid. § 201(b) (2012). Thus, it was improper for the judge to take judicial notice of it. As it is not supported by any evidence it too should be set aside.

The judge went on to find that because of the high number of cell towers, the location revealed by triangulation is as precise as GPS (CA.123). She specifically reasoned that to accept the Commonwealth's argument that CSLI does not reveal a precise location

> this Court would have to close its eyes to reality: as cell phones become ubiquitous, cell towers too have proliferated and, through a process of "triangulation" among different towers, CSLI is now no less accurate than GPS in pinpointing location (except perhaps in remote rural areas).

(CA.123). There was a dispute at the hearing as to whether historic CSLI can reveal the exact location of a cell phone user. There was no evidence presented at the hearing about GPS and the similarities or difference between it and CSLI. The CSLI record at issue was never entered into evidence or brought before the judge. Thus, there was no basis for the judge to find that historic CSLI was as accurate as GPS in pinpointing location.

Moreover, there was no evidence about triangulation presented at the hearing. While triangulation generally can be defined as the "process of determining the coordinates of point based on the known location of two other points," there are

different ways to triangulate cell towers to obtain a location and each way varies in the precision of the location it reveals. Smith, *supra*, at 3.[5] Here, there was no evidence to support that triangulation was used at all, never mind that the type of triangulation that was used was one that would reveal a precise location. Therefore, it was improper for the judge to find that triangulation occurred at all in this instance.

Again, it was the defendant's burden to support his claim with evidence. He did not. The judge simply relieved the defendant of his burden when she improperly took judicial notice of facts in order to support her ruling that CSLI revealed as precise of a location as GPS. This was clear error. Accordingly, the judge's order must be reversed.

II. THE JUDGE ERRED BECAUSE THE DEFENDANT FAILED TO SHOW THAT A SEARCH IN THE CONSTITUTIONAL SENSE OCCURRED.

The judge also erred in ruling that the Fourth Amendment to the United States Constitution or art. 14

---

[5] "'Triangulation' in this context refers to a range of techniques for more precisely locating a cellular subscriber handset by comparing the radio signal received from the handset at multiple vantage points." 111 Cong. at 138 (statement of Blaze). Some of these techniques use the angle the radio signal arrives at different points while some use the time the signal arrives at certain points. 111 Cong. at 138 (statement of Blaze).

of the Massachusetts Declaration of Rights were implicated by the government's request and receipt of historic CSLI from the defendant's cell service provider. Not every search and seizure implicates the Fourth Amendment or art. 14. *See Commonwealth v. Molina*, 459 Mass. 819, 824 (2011) (quoting *Commonwealth v. Porter P.*, 456 Mass. 254, 259 (2010)) (In deciding whether a search violated the Fourth Amendment and art. 14 the must "'first determine whether a search in the constitutional sense took place.'"). Instead, it is the defendant's burden to demonstrate: (1) that the search or seizure was "conducted by" or was "at the direction of the state," *District Attorney for the Plymouth District v. Coffey*, 386 Mass. 218, 220-221 (1982); (2) that he has standing to challenge the search; and (3) that he has a reasonable expectation of privacy in either the place searched or the items seized. *See Commonwealth v. Mubdi*, 456 Mass. 385, 390, 392 (2010). Here, the defendant failed to show that the Commonwealth was involved in the creation or retention of CSLI or that he has any expectation, reasonable or otherwise, in it.

A. The Defendant Failed To Show That The Surveillance Was By Or At The Direction Of The Commonwealth.

The origin and history of the Fourth Amendment "'clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies.'" *Coffey*, 386 Mass. at 221 (quoting *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921)). "The same considerations apply to art. 14." *Id*. To show that a constitutional search occurred the defendant must demonstrate that the government either conducted the search or directed another to conduct the search. *Compare id*. at 222 (constitutional question not raised because there was no evidence that Commonwealth directed phone company to install a pen register) with *District Attorney for the Plymouth District v. New England Tel. & Tel. Co.*, 379 Mass. 586, 590 (1980) (constitutional question raised because the Commonwealth directed the phone company to install a pen register).

The facts of *Coffey* illustrate this point. In *Coffey*, the victim requested that the phone company install a cross frame unit trap on her telephone line to trace annoying phone calls she had been receiving. 386 Mass. at 219. Three phone calls were traced back

to the defendant. *Id*. The defendant moved to suppress the record of these calls alleging that his Fourth Amendment and art. 14 rights had been violated. *Id*. at 220. This Court rejected that claim explaining that the Fourth Amendment and art. 14 were not implicated because the Commonwealth had no involvement in the creation of the records. *Id*. at 221.

Here too, the Commonwealth had no involvement in the collection of the CSLI. Cell phone service providers maintain these records independently in their ordinary course of business for business purposes such as improving service and determining roaming charges based on the cell site that a subscriber's phone uses for a particular call. *See In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't*, 534 F. Supp. 2d at 590; *In re United States Orders pursuant to 18 U.S.C. 2703(d)*, 509 F. Supp. 2d 76, 78 (D. Mass. 2007).

That the CSLI already existed independent of any governmental action also differentiates this case from a more modern electronic surveillance case like *Commonwealth v. Rousseau*, 465 Mass. 372, 832 (2013). In *Rousseau* this Court considered whether an individual had standing to challenge the attachment of

a GPS device to a car in which he was a passenger and had no possessory interest in. 465 Mass. at 382. This Court held 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*. (italics added). In that case it was clear that there was government action because the police took a GPS device, put it on a truck, and then electronically surveilled the defendant's location from the attached device.

Here, in contrast, the government did not take any action that caused Sprint, the defendant's cell service provider, to record the defendant's CSLI. Cell service providers collect the information without a request or order from the government. The government does not require a cell service provider to collect this type of information and does not dictate how long they must store it. Cell service providers collect such information for routine business purposes. It cannot be said then that any governmental action caused the defendant's location through CSLI to be recorded. "In the case of . . . historical cell site information, the Government merely comes in after the fact and asks a provider to

turn over records the provider has already created." *In re Smartphone Geolocation Data Application*, No. 13-MJ-242 (GRB), 2013 U.S. Dist. LEXIS 62605, *33 (E.D. N.Y. May 1, 2013). Thus, the motion judge erred because there was no search under the Fourth Amendment or art. 14.

B. The Defendant Failed To Show That He Had An Expectation Of Privacy In CSLI Because It Is A Third Party Business Record And It Does Not Reveal Any Protected Information.

The judge also erred in allowing the defendant's motion to suppress because the defendant failed to demonstrate that he had any expectation of privacy in CSLI. To meet this burden, the defendant must demonstrate that he "exhibited an actual (subjective) expectation of privacy," and that this "expectation [is] one that society is prepared to recognize as objectively reasonable." *Katz v. United States*, 389 U.S. 347, 361 (1967); *accord Commonwealth v. Morrison*, 429 Mass. 511, 513-514 (1999). If the record is unclear, it is the defendant, not the Commonwealth, who has failed to meet the burden of proof. *See Commonwealth v. Netto*, 438 Mass. 686, 697 (2003) ("the burden is initially on the defendants to demonstrate that they had a reasonable expectation of privacy.).

The Supreme Court has yet to rule on whether the search of CSLI implicates the Fourth Amendment. The majority of courts to consider this issue have ruled that the acquisition of historic CSLI pursuant to a 2703(d) order does not implicate the Fourth Amendment because it is a business record held by a third party. *See, e.g.*, *In re: Application of the United States of America for Historical Cell Site Data*, No. 11-20884, 2013 U.S. App. LEXIS 15510 (5th Cir. July 30, 2013); *United States v. Caraballo*, No. 5:12-cr-105, 2013 U.S. Dist. LEXIS 112739, *53 (D. Vt. Aug. 7, 2013); *United States v. Rigmaiden*, No. 08-814-PHX-DGC, 2013 U.S. Dist. LEXIS 65633, *32-33 (D. Ariz. May 8, 2013); *United States v. Wilson*, NO. 1:11-CR-53-TCB-ECS-3, 2013 U.S. Dist. LEXIS 37783, *17 (N.D. Ga. Feb. 20, 2013); *United States v. Steve Ruby*, NO. 12CR1073 WQH, 2013 U.S. Dist. LEXIS 18997, *17 (S.D. Cal. Feb. 12, 2013); *In re Application of United States for Order Pursuant to 18 U.S. C. 2703(d)*, 849 F. Supp. 2d 177, *179 (D. Mass. 2012); *United States v. Madison*, No. 11-60285, 2012 U.S. Dist. LEXIS 105527, *29-30 (S.D. Fla. July 30, 2012); *United States v. Velasquez*, No. 08-730-WHA, 2010 U.S. Dist. LEXIS 118045, *17-18 (N.D. Cal. Oct. 22, 2010); *United States v. Dye*, No. 10CR221, 2011 U.S. Dist. LEXIS 47287, *25-26 (N.D.

Ohio Apr. 27, 2011); *United States v. Benford*, No. 09 CR 86, 2010 U.S. Dist. LEXIS 29453, *7-8 (N.D. Ind. Mar. 26, 2010); *United States v. Suarez-Blanca*, No. 07-023-MHS/AJB, 2008 U.S. Dist. LEXIS 111622, *27-28 (N.D. Ga. Mar. 26, 2008).

Other courts have held that the acquisition of historic CSLI without a warrant violates the Fourth Amendment if the record covers a long period of time because the extent of long-term electronic monitoring reveals an individual's movements, which implicates an individual's legitimate expectation of privacy. *See, e.g., In the Matter of an Application of the United States of American for an Order Authorizing Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011); *In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, 736 F. Supp. 2d 578, 579 (E.D.N.Y 2010). Neither theory, however, supports a conclusion that the acquisition of CSLI in this case violated either the Fourth Amendment or art. 14.

1. An Individual Has No Subjective or Objective Expectation of Privacy in CSLI Because It Is A Business Record Created, Held, And Owned By A Third Party.

CSLI is information that was created and maintained by a third party. *See In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't*, 534 F. Supp. 2d at 590; *In re United States Orders pursuant to 18 U.S.C. 2703(d)*, 509 F. Supp. 2d at 78. The Supreme Court "has repeatedly held that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Smith v. Maryland*, 442 U.S. 735, 744 (1979). Under the "third party doctrine," the disclosure of information to a third party does not implicate the Fourth Amendment even if the information is disclosed under "the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Graham,* 846 F. Supp. 2d 384, 397 (D. Md. 2012) (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)). The reasoning underlying the third party doctrine is that, in voluntarily disclosing information to a third party, an individual assumes a certain risk that the third party will in turn reveal the information to a

government agency. *Miller*, 425 U.S. at 443. Moreover, when the information is proprietary to, and in the possession of, the third party, the privacy interest in the information is even further diminished.[6] In the present case, the third party doctrine forecloses any claim by defendant that he has an objectively reasonable privacy interest in CSLI.

The reasoning in *Smith v. Maryland*, 442 U.S. 735 (1979), is analogous and applicable here.[7] In *Smith*, the issue was whether a pen register, installed at the phone company's central office to monitor phone calls made from the suspect's home phone, constituted a "search" under the Fourth Amendment. *Smith*, 442 U.S. at 736-737. In concluding that an individual does not

---

[6] In *Miller*, the Supreme Court held that the compelled disclosure of respondent's financial records from two banks did not constitute a Fourth Amendment search. 425 U.S at 442-443. In rejecting the respondent's Fourth Amendment challenge, the Court held that bank records are the "business records of the banks," not the "respondent's private papers." *Id.* at 442. As a result, the respondent could "neither assert ownership nor possession" in the bank records. *Id.*

[7] Massachusetts cases have similarly held that an individual does not have an expectation of privacy in information voluntarily turned over to third parties. *See, e.g.*, *Commonwealth v. Buccella*, 434 Mass. 473, 483 (2001); *Commonwealth v. Cote*, 407 Mass. 827 (1990) (no reasonable expectation of privacy in telephone message records); *Commonwealth v. Feodoroff*, 43 Mass. App. Ct. 725 (1997) (no reasonable expectation of privacy in telephone company billing records).

have an expectation of privacy in the numbers that he dials from his phone, the Court stated, "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id*. at 742. Further, the Court held that telephone users "typically know that . . . the telephone company has facilities for recording [the numbers they dial] and that the phone company does in fact record this information for a legitimate business purpose." *Id*. at 743.

Here, the judge rejected the third party doctrine and distinguished the case at bar from both *Smith* and *Miller* by explaining that unlike a telephone which a user must affirmatively dial, "there is no overt or affirmative act by the user" of a cell phone, "whereby she voluntarily exposes her location to a third party: CSLI is generated automatically without the cell phone user's participation beyond the act of receiving or making a call" (CA.124). She went on to explain that "CSLI can be generated even without a call being made since, through a process of 'registration,' a cell phone will periodically identify itself to a cell

tower whenever a phone is on, whether a call is made or not" (CA.124).

That reasoning is flawed for two reasons. First, it is not supported by any evidence. Again, the cell tower records were not before the judge in this case. There was nothing to show that registration data was ever sent to the Commonwealth. There is nothing to show that registration data is typically turned over when cell service providers respond to 2703(d) orders. "While retention practices vary by carrier, many retain registration data only for about 10 minutes, unless the cell phone has registered again at the same or another cell tower." *In re United States ex rel. an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 534 (D.Md. 2011) (citing FTC Workshop, "Introduction to Privacy and Security Issues Panel" (Dec. 12, 2000), available at http://www.ftc.gov/bcp/workshops/wireless/001212.htm). Indeed, commenters have also noted that it is unclear that such information even could be turned over. *See* Recent Development, Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, 18 Harv. J. Law & Tec 307, 309 (2004) ("It is unclear, however, whether cell service

providers maintain records of these registrations."); Jen Manso, "Cell-Site Location Data and the Right to Privacy," 27 Syracuse Sci. & Tech. L. Rep. 1, 4 (2002) ("If registration data were also collected by the provider and made available").

Second, the judge applied an incorrect standard when assessing whether the defendant had an expectation of privacy. In *Smith*, the Supreme Court cautioned against "an assumption of ignorance" on the part of the telephone customer, *see Graham*, 846 F. Supp. 2d at 401, by assuming that the user was familiar with both the technology used and with the fact that the phone company "has facilities for making permanent records of the numbers that they dial, for they see a list of their long-distance (toll) calls on their monthly bills." 442 U.S. at 742. The Court further explained that, "[t]he switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber." *Id*. at 744. As in *Smith*, this assumption should apply to the cell phone customer. Cell towers are simply the modern counterpart of the technology employed by the telephone company in *Smith*. Thus, the appropriate analysis here is whether an individual with a

reasonable understanding of the technology had an objective expectation of privacy in CSLI.

The answer to that question, as the majority of courts have ruled, is no. *See, e.g.*, *In re: Application of the United States of America for Historical Cell Site Data*, 2013 U.S. App. LEXIS 15510 at *37; *United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012); *Dye*, 2011 U.S. Dist. LEXIS 47287 at *25-26; *Velasquez*, 2010 U.S. Dist. LEXIS 118045 at *17-18; *Benford*, 2010 U.S. Dist. LEXIS 29453 at *8; *Suarez-Blanca*, 2008 U.S. Dist. LEXIS 111622 at *29-30. "[A] cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call." *In re: Application of the United States of America for Historical Cell Site Data*, 2013 U.S. App. LEXIS 15510 at *35; *accord In Re Smartphone Geolocation Data Application,* 2013 U.S. Dist. LEXIS 62605 at *46 ("it is clearly within the knowledge of cell phone users that their telecommunications carrier, smartphone manufacturer and others are aware of the location of their cell phone at any given time"); *Madison*, 2012 U.S. Dist. LEXIS 105527 at *26-27 ("[C]ell-phone users have knowledge that when they place or receive a calls, they, through their cell

phones, are transmitting signals to the nearest cell tower, and, thus, to their communications service providers."). The habit of looking at one's phone to see the strength of the signal, illustrated by the now iconic "bars," demonstrates an understanding by cell phone users that their cell phone is constantly accessing, or attempting to access, a service provider's towers even when the phone is not in use. Likewise, using a map or weather function on the phone equally requires locational data that the user must provide. Cell service providers, including Sprint in its Privacy Policy, also inform customers that they maintain such location data.[8]

Further, the defendant's use of his cell phone was entirely voluntary. He was not "require[d] as a member of the public to own or carry a phone." *In re: Application of the United States of America for Historical Cell Site Data*, 2013 U.S. App. LEXIS 15510

---

[8] The Sprint Privacy Policy states, in relevant part: We may collect information about your device such as the type, version of operating system, signal strength, whether it is on and how it is functioning, as well as information about how you use the device and services available through it, such as your call and data usage and history, *your location*, web sites you have visited, applications purchased, applications downloaded or used. *http://www.sprint.com/legal/privacy.html* (last visited August 7, 2013) (emphasis added).

at *37. He was not required to "obtain his cell phone service from a particular service provider that keeps historical cell site records for its subscribers, either." *Id*. at *37-38. He was not required "to make a call, let alone to make a call at a specific location." *Id*. at *38. "Because a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, [and] the provider retains this information . . . he voluntarily conveys his cell site data each time he makes a call." *Id*. at *39. The defendant is such a cell phone user. When he voluntarily chose to use his cell phone he, like phone users since *Smith*, assumed the risk that his cell service provider could turn over information obtained through that use. Thus, the judge's ruling should be reversed.

2. The Defendant Failed To Demonstrate A Subjective Or Objective Expectation Of Privacy In The Location That CSLI Revealed.

The Supreme Court has never applied the standards applicable to electronic surveillance cases, *see, e.g.*, *United States v. Karo,* 468 U.S. 705, 714-715 (1984), *United States v. Knotts*, 460 U.S. 276, 282 (1983), to cases that involve the disclosure of business records from a third party through a judicial

order. *See, e.g.*, *Smith*, 442 U.S. at 745-846; *Miller*, 425 U.S. at 443. This is true even though such records, like a pen register, could reveal an individual's location. Unlike an electronic surveillance case, the conduct here involved only looking at a record, which was generated solely by the cell service provider in its ordinary course of business, and was never in the defendant's possession. Hence, such records could never be considered "private" in the sense of ownership. In signing up and using Sprint's network the defendant took the risk that the information he provided them would be revealed to the government. *See Miller*, 425 U.S. at 443; *accord Feodoroff*, 43 Mass. App. Ct. at 730. There is simply no reason, on these facts, to distinguish CSLI from any other business record.

Other courts, however, have analyzed whether the defendant has a reasonable expectation of privacy in CSLI under the Supreme Court electronic surveillance cases of *Knotts* and *Karo*. In *Knotts*, the Court explained that electronic surveillance which reveals an individual's public movements does not violate the Fourth Amendment because "nothing . . . prohibit[s] the police from augmenting the sensory faculties bestowed upon them at birth with such enhancements as

science and technology afforded them in this case." 460 U.S. at 282. In *Karo*, the Court held that Electronic surveillance which reveals an individual's movements inside "a location not open to visual surveillance," does, however, violate the Fourth Amendment because it allows the police to obtain information "it could not have otherwise obtained without a warrant." 468 U.S. at 714-715.

Among courts to have analyzed CSLI in this way several have come to the conclusion that the acquisition of such data does not violate the Fourth Amendment because CSLI does not reveal a precise location. *See, e.g., In re Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304, 312-13 (3d Cir. 2010); *Suarez-Blanca,* 2008 U.S. Dist. LEXIS 111622 at *9-11; *In re United States for Order for Prospective Cell Site Location Info.*, 460 F. Supp. 2d at 462 (noting that if such information could track an individual into a private home then it might raise Fourth Amendment concerns). As noted here, the actual CSLI record was never entered into evidence. It was never before the motion judge and is not before this Court. Therefore, it cannot be said on this

record that the defendant's Fourth Amendment or art. 14 rights were violated because the CSLI in this instance revealed any particular location, either public or private, because there is no evidence whatsoever as to what location was actually revealed. It is the defendant's burden to prove that he had a subjective and objective expectation of privacy in the location revealed. He did not meet this burden. For this reason alone, his motion should have been denied.

Further, in so far as the defendant's location was generally revealed by this data, the defendant has not demonstrated or even asserted, that he had a reasonable expectation of privacy in it, *see Karo*, 468 U.S. at 714, or that he had a reasonable expectation that his location would not be so revealed. *See Knotts*, 460 U.S. at 281 (no reasonable expectation of privacy in his movements from one place to another); *Katz*, 389 U.S. at 361 (an individual has no expectation of privacy in what is revealed to the public). Notably, his affidavit did not include any assertion about the cell records revealing a location in which he enjoyed an expectation of privacy (CA.11). For that reason too, his motion should have been denied.

The Supreme Court recently revisited the constitutionality of electronic surveillance in *Jones*, when it considered whether the installation of a GPS device on the defendant's car and the subsequent use of the device to monitor the vehicle's movements constituted an unreasonable search. 132 S. Ct. at 949-950. Holding that it did, the Court's ruling rested on the fact that the government's installation of the GPS device on the suspect's car constituted a trespass. *Id*. The Court reasoned that, "[t]he government physically occupied private property for the purpose of obtaining information" and as a result, these actions constituted a search within the meaning of the Fourth Amendment. *Id*. For that reason the Court did not engage in the familiar *Katz* analysis and ask whether the defendant had an expectation of privacy in his location because the installation of the GPS involved a physical trespass, which necessarily violated the defendant's right to privacy in his car. *Id*. at 952. The Court explained further, however, that electronic surveillance without such a trespass would still be subject to the *Katz* analysis but reserved for another day the question of whether long-term electronic surveillance that does not

involve a trespass would violate the Fourth Amendment. *Id*. at 954-955.

This Court, in *Rousseau*, recently considered under art. 14, whether a passenger, who had no possessory interest in the car, had standing to challenge the installation of a GPS and the electronic surveillance of that car. 465 Mass. 382. The issue framed by this Court was not, as it had been by the Supreme Court in *Knotts* and *Karo*, whether the defendant had a reasonable expectation of privacy in the location that was revealed by the electronic surveillance but rather whether the defendant had a reasonable expectation of privacy in not being so surveilled. *Id*. at 382 (court must decide "whether, even in the absence of a property interest, the government's contemporaneous monitoring of one's comings and goings in public places invades one's reasonable expectation of privacy."). Answering that question under the traditional *Katz* formulation, this Court held "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 the showing of probable cause." *Id*.

Applying the holding of *Rousseau* to the facts of the case at bar it becomes clear that the acquisition of CSLI through a 2703(d) order does not violate art. 14. First, the holding in *Rousseau* specifically contemplates whether an individual had an expectation of privacy to not be electronically surveilled by GPS. *See id*. (asks whether an individual "may reasonably expect not to be subjected to extended GPS electronic surveillance"). That means the issue to be decided here is whether an individual may reasonably expect that his cell phone records, which detail where his cell phone connected within the cell network and were compiled and kept by his cell service provider, would not be disclosed. As discussed above, the defendant had no such expectation.

The holding in *Rousseau* also instructs that the electronic surveillance has to be by the government, targeted at the defendant's movements, and not subject to judicial oversight. Here, the surveillance was neither conducted by the government nor specifically targeted at the defendant's movements. Sprint collects this type of data in its normal course of business. Cell service providers generally do so for business purposes such as improving cell reception and service and determining roaming charges. *See In re*

Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't, 534 F. Supp. 2d at 590. Those purposes have nothing to do with tracking an individual's movements or location.

Importantly, the search was subject to judicial oversight. "'It is well known that art. 14 was adopted to prohibit the abuse of official power brought about by two devices which the British Crown used in the colonies: the general warrants and the writs of assistance,'" which allowed the government to search with almost unlimited discretion. *Commonwealth v. Valerio*, 449 Mass. 562, 566 (2007) (quoting *Jenkins v. Chief Justice of the Dist. Court Dep't*, 416 Mass. 221, 229 (1993)). Here, however, the situation presented is not the typical "warrantless" search. Prior to obtaining these records the government had to apply for a 2703(d) order, which laid out "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other material sought, are relevant to an ongoing criminal investigation." 18 U.S.C. § 2703(d). After doing so, a judge issued the order and the government served it upon the cell service provider, who then complied with the order and sent the historic CSLI

record to the government. That process is different than the police entering an individual's home without a warrant and searching it or physically placing a device on a car and tracking it in real time. It cannot be said then that this type of search was undefined and limitless, the very vice art. 14 was designed to prevent. *See Commonwealth v. Balicki*, 436 Mass. 1, 8 (2002).

Additionally, it was also an error for the judge to rule that "the duration of the monitoring is irrelevant" (CA.125). In *Jones*, Justice Alito, in a concurrence joined by Justices Kagan, Breyer, and Ginsburg, stated that short-term monitoring of an individual's movements on public streets "accords with expectations of privacy that our society has recognized as reasonable." *Id*. at 964 (Alito, J., concurring). However, longer term GPS monitoring "impinges on expectations of privacy." *Id*. Likewise, in *Rousseau*, this Court noted that while not necessary to "decide how broadly such an expectation might reach and to what extent it may be protected," under art. 14, the fact that the police monitored the defendant over a thirty day period was sufficient to establish an expectation of privacy. 465 Mass. at 382. Both decisions inform that contrary to the judge's ruling

the length of surveillance is important to the expectation of privacy analysis.

Here, the Commonwealth was authorized to obtain historic CSLI for the period of August 24, 2004 through September 7, 2004. Unlike the data generated from a GPS tracking device that is planted on a vehicle, historic CSLI does not involve ongoing, real-time monitoring. Historic CSLI is simply information regarding past events that is collected and recorded by a third party cell service provider, and in turn, obtained by the government after the fact. It does not involve the real-time monitoring of the defendant's movements from location to location that this Court and Justice Alito was concerned with.

A number of federal courts have also held that an individual has a Fourth Amendment privacy interest in the contents of CSLI because of the long-term nature of the surveillance. *See, e.g.*, *In the Matter of an Application of the United States of American for an Order Authorizing Release of Historical Cell-Site Information*, 809 F. Supp. 2d at 114 (requesting CSLI for a 113 day period); *In Re Application of the United States of America for Historical Cell Cite Data*, 747 F. Supp. 2d at 828 (requesting CSLI for a 60 day period); *In the Matter of an Application of the United*

States of America for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d at 579 (requesting CSLI for a two month period).

These cases, however, rely upon an analytical approach articulated by the Court of Appeals for the District of Columbia Circuit in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010). In *Maynard*, the court held that an individual has a legitimate privacy interest in cell site location information that is *cumulative.*[9] 615 F.3d at 555-68. Under this theory, an individual who ordinarily would not have a reasonable expectation of privacy over his location while making a specific trip would have a reasonable expectation of privacy in the totality of his movements over a long period of time. *Id.*

Under the present facts, the *Maynard* cumulative CSLI approach does not apply because the CSLI obtained does not cover the long term time frames that were at issue in the cases cited above. The federal cases listed are limited to their facts. Had the CSLI acquired by the government in the above cases been limited to the short time period at issue here, the

---

[9] Cumulative cell site location information is that which is obtained by way of continual or long-term surveillance of an individual's CSLI. *See Maynard*, 615 F.3d at 555-68.

reasoning of the cases suggests that the outcomes would have been different. Moreover, the court in *Maynard* specifically noted that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. This type of information can each reveal more about a person than does any individual trip viewed in isolation." 615 F.3d at 561. Such information was simply not obtained here.

Finally, the Fourth Amendment and art. 14 need to strike "a balance between the individual citizen's interest in conducting certain affairs in private and the general public's interest in subjecting possible criminal activity to intensive investigation." *Reporters Committee for Freedom of Press v. American Tel. & Tel. Co.*, 593 F.2d 1030, 1042-1043 (D.C. Cir. 1978). To meet this end, it "secur[es] for each individual a private enclave a 'zone' bounded by the individual's own expectations of privacy." *Id*. at 1043. Of course, in normal life an individual must "transact with other people" and in doing so leaves behind evidence of his activities. *Id*. "To the extent that an individual knowingly exposes his activities to third parties, he surrenders Fourth

Amendment protections, and, if the Government is subsequently called upon to investigate his activities for possible violations of the law, is free to seek out those third parties, to inspect their records, and to probe their recollections for evidence." *Id*. In that way, "the Fourth Amendment carries with it both a promise and a warning." *Id*. It promises a zone of privacy "shielded from unwarranted investigative scrutiny." *Id*. Yet, it also warns "each individual that, once he projects his activities beyond this private enclave, the Government is free to scrutinize them for law enforcement purpose." *Id*.

Thus, where the defendant has not shown that the surveillance in this instance intruded into a private zone or mapped out his movements to an invasive degree the acquisition of CSLI through a court order simply did not violate the Fourth Amendment or art. 14. For this reason, the judge's order must be reversed.

III. ALTERNATIVELY, THE EXCLUSIONARY RULE SHOULD NOT APPLY BECAUSE THE GOVERNMENT DID NOT GAIN ACCESS TO THIS INFORMATION THROUGH ANY MISCONDUCT.

The motion judge also erred because, even if the defendant demonstrated a reasonable expectation of privacy in CSLI, the exclusionary rule should not apply. The general rule is that evidence is to be excluded if it is found to be the 'fruit' of a police

officer's unlawful actions." *Commonwealth v. Balicki*, 436 Mass. 1, 15 (2002) (citing *Wong Sun v. United States*, 371 U.S. 471, 484 (1963)). "[E]xclusion 'has always been [the Court's] last resort, not [the Court's] first impulse.'" *Herring v. United States*, 555 U.S. 135, 142 (2009) (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)). "The decision whether to exclude such evidence should properly turn on: (1) the degree to which the violation undermined the principles underlying the governing rule of law, and (2) the extent to which exclusion will tend to deter such violations from being repeated in the future." *Commonwealth v. Sbordone*, 424 Mass. 802, 809-810 (1997) (citing *Commonwealth v. Gomes*, 408 Mass. 43, 46 (1990)). The target of the exclusionary rule is police misconduct. *See Commonwealth v. Brandwein*, 435 Mass. 623, 632 (2002). "[U]nless there is either police misconduct, or police instigation of misconduct by a private party, there is no 'poisonous tree' that can taint subsequent police investigation. *Id*. at 633.

Here, there was no police misconduct. "'[A]n assessment of the flagrancy of the police misconduct constitutes an important step in the calculus' of applying the exclusionary rule." *Herring*, 555 U.S. at

143 (quoting *United States v. Leon*, 468 U.S. 897, 911 (1984)). "[E]vidence should be suppressed 'only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment.'" *Illinois v. Krull*, 480 U.S. 340, 348-349 (1987) (quoting *United States v. Peltier*, 422 U.S. 531, 542 (1975)). Here, there was no violation of the law. The law regarding Fourth Amendment and art. 14 protections for historical CSLI is in flux. To this date, neither our Supreme Judicial Court nor the United States Supreme Court has directly addressed the issue. Certainly, in 2004, when the 2703(d) order was obtained in this case, no court or law stated that a search warrant was required to obtain historic CSLI. The officers in this case did not undermine the governing rule of law but rather, acted in accordance with the statutory scheme that was in place then and now. The officers followed the legal process in order to obtain the information they sought.

Second, exclusion of this evidence will not deter violations from being repeated in the future. There is no evidence here that investigators engaged in conduct designed to avoid having to obtain a warrant. To the contrary, the officers followed the statutory

scheme when they obtained the order. *See Krull*, 480 U.S. at 349-350 ("Unless a statute is clearly unconstitutional, an officer cannot be expected to question the judgment of the legislature that passed the law.") The Stored Communications Act, in place since 1986, cannot reasonably be said to be of the sort that is clearly unconstitutional on its face. Here, the records were sought in full conformity with the statute, subject to prior judicial oversight. No deterrent effect would flow from the exclusion of this evidence, as the officers acted within the parameters of the law.

Additionally, contrary to the judge's finding, (CA.116), the Commonwealth argued that, while not required, the affidavit submitted to the court with the application for a 2703(d) order established probable cause to believe that CSLI from the defendant's cell phone would furnish evidence relative to the investigation into the disappearance of Julaine Jules (CA.57). Trooper McCauley's affidavit stated that

> Jules disappeared on August 24, 2004 and was reported missing by her father on August 25, 2004. She was last seen at Circles, located at 300 Congress Street in Boston, where she was employed as a credit card concierge. At approximately 12:20 AM on August 25, Jules' vehicle was found burning on the

> Malden/Revere line. Jules' body was discovered on September 19, 2004 when it appeared, wrapped in plastic, on the Cambridge side of the Charles River. An investigation into Jules' death revealed that Jules had two boyfriends —one of which was the defendant. The weekend preceding Jules' disappearance, on August 21-22, the other boyfriend was visiting Jules in Boston.
>
> The defendant was interviewed by Trooper McCauley and her partner, Pi Heseltine on August 28, 2004. The defendant admitted to having his cousin, Melissa Mitchell, contact Jules and contact a rouse in order to lure Jules to the defendant's residence on the date of Jules' disappearance. As the troopers began to question the defendant about whether he would appear on any surveillance tape near where Jules disappeared, he began to cry and moan. A subsequent interview with Mitchell revealed information that the defendant contacted Mitchell on August 25, 2004 and reported that Jules had come to his residence and that she was a little upset, but that overall things went well. Mitchell also informed the troopers that on August 26, 2004, the defendant contradicted himself and told Mitchell that he actually had not seen Jules on August 24. Troopers McCauley and Haseltine had an opportunity to examine the phone records of both Jules and the defendant, and it was their belief, based on their training, that the historic CLSI would show the general location of both Jules and the defendant during the night of August 24, 2004 and early morning of August 25, 2004.

(CA.57). These facts sufficiently set forth probable cause to believe that CSLI would reveal information

relative to the murder investigation. Because of that, the exclusionary rule should not apply.

Finally, the "ultimate touchstone" of the Fourth Amendment and art. 14 is reasonableness. *Commonwealth v. Entwistle*, 463 Mass. 205, 213 (2012); *accord Commonwealth v. Townsend*, 453 Mass. 413, 425 (2009). Here, the police acted reasonably. They applied for a court order to obtain a business record from a cell service provider under 2703(d) because in 2004, there was no Massachusetts statute or case that said otherwise. Though a 2703(d) order need only be supported by an affidavit that establishes "specific and articulable facts," the police provided an affidavit that established probable cause to believe that CSLI would reveal evidence relative to the murder investigation. Not only did the officers follow the statutory scheme, but because the affidavit met the probable cause standard required for a search warrant, a search warrant would have issued had the Commonwealth sought one. Accordingly, as the very purpose of the exclusionary rule is not served by the suppression in this instance, the judge erred in ruling that it should apply. Thus, her order should be reversed.

CONCLUSION

For the foregoing reasons, the Commonwealth respectfully requests that this Honorable Court reserve the allowance of the defendant's motion to suppress.

Respectfully submitted
FOR THE COMMONWEALTH,

DANIEL F. CONLEY
District Attorney
For the Suffolk District

CAILIN M. CAMPBELL
Assistant District Attorney
BBO# 676342
One Bulfinch Place
Boston, MA 02114
(617) 619-4070
Cailin.campbell@state.ma.us

AUGUST 2013

ADDENDUM

G.L. c. 265, § 1. Murder defined.

Murder committed with deliberately premeditated malice aforethought, or with extreme atrocity or cruelty, or in the commission or attempted commission of a crime punishable with death or imprisonment for life, is murder in the first degree. Murder which does not appear to be in the first degree is murder in the second degree. Petit treason shall be prosecuted and punished as murder. The degree of murder shall be found by the jury.

18 U.S.C. § 2703. Required disclosure of customer communications or records.

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

(b) Contents of Wire or Electronic Communications in a Remote Computing Service.—

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

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

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

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

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

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

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

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

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

(c) Records Concerning Electronic Communication Service or Remote Computing Service.—

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

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

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

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

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

(E) seeks information under paragraph (2).

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

(A) name;

(B) address;

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

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

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

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

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a

Federal or State grand jury or trial subpoena or any means available under paragraph (1).

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

(d) Requirements for Court Order.— A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter.— No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement To Preserve Evidence.—

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

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

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