

34

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CRIMINAL ACTION
NO. 11-10748

COMMONWEALTH

v.

SHABAZZ AUGUSTINE

MEMORANDUM OF DECISION AND ORDER
ON THE DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

The defendant is charged with murdering his girlfriend Julaine Jules. She disappeared on August 24, 2004; her body was discovered in the Charles River almost a month later. Because of the location of her body, Jules' death was originally investigated by the Middlesex County District Attorney's Office. In the course of that investigation, prosecutors obtained certain cell phone information regarding the defendant's location around the time of his girlfriend's disappearance. The investigation was subsequently transferred to Suffolk County and in 2011, the defendant was charged with killing Jules. The case is now before the Court on the defendant's Motion to Suppress the cell phone information on the grounds that it was obtained without a warrant and without probable cause. Because I conclude that the government's access to this kind of information amounts to a search under article 14 of the United States Declaration of Rights, I conclude that the motion must be Allowed.¹

¹With the trial date looming, this Court endorsed the Motion as allowed on February 26, 2013. This memorandum explains the Court's reasoning.

R

BACKGROUND

Because there was no dispute as to the relevant facts, this Court did not hold an evidentiary hearing. Nevertheless the motion does require some factual context as to the technology at issue.² Unlike conventional land line 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 through 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.

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

² The parties agreed that this Court could take "judicial notice" of facts relating to this technology. See Commonwealth v Lykus, 367 Mass. 191, 203 (1975). Those facts are succinctly described in 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) as well as In re Application of United States of America for Historical Cell Site Data, 747 F.Supp.2d 897 (S.D.Tex. 2010).

exactitude, thus diminishing the difference between CSLI and the Global Positioning System, or GPS.

Under the Stored Communications Act (SCA) the government can require a provider of an electronic communication service to disclose "a record or other information pertaining to a subscribed customer of such services (not including the contents of communications)" by obtaining a judicial order. 18 U.S.C. §2703(c)(1). To get such an order, the government must demonstrate to a court "specific and articulable facts showing that there are reasonable grounds to believe that the contents of wire or electronic communication or the record or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. §2703(d). In the instant case, the Middlesex County District Attorney's office on September 24, 2004 applied for and obtained such an order for phone number 617-905-7830, the cell phone that police had determined was being used by the defendant during the relevant time. The order that issued allowed the Commonwealth to access CSLI for that number between August 24, 2004 and September 7, 2004.

DISCUSSION

There is no dispute that the Commonwealth's request for CSLI in the instant case complied with the SCA. It is equally undisputed that there was no search warrant accompanying the application. Nor does the government argue that the affidavit submitted in support of the request under the SCA contains enough facts to amount to probable cause. A warrant and probable cause would be necessary only if this Court concludes that government access to this CSLI constitutes a "search" for constitutional purposes. This Court concludes that, at least under

article 14 of the Massachusetts Declaration Rights, there was a search such that this information must be suppressed.

To date, neither the Supreme Judicial Court nor the Appeals Court has opined on the question of whether government access to CSLI infringes on one's reasonable expectation of privacy under article 14. Similarly, the United States Supreme Court has not directly addressed the question under the Fourth Amendment. Beginning in 2004, however, lower federal courts have wrestled with the question, with the majority concluding that, so long as the government complied with the SCA, nothing further was required. See e.g., In re Application of U.S., 509 F.Supp.2d 76, 80 (D.Mass.2007), *reversing*, 509 F.Supp.2d 64 (D.Mass. 2007); United States v. Ruby, 2013 WL 544888, at *6 (S.D.Cal. Feb. 12, 2013); United States v. Graham, 846 F.Supp.2d 384, 390 (D.Md. 2012); United States v. Dye, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011); United States v. Velasquez, 2010 WL 4286276, at *5 (N.D.Cal. Oct. 22, 2010); United States v. Benford, 2010 WL 1266507, at *3 (N.D.Ind. Mar. 26, 2010); United States v. Suarez-Blanca, 2008 WL 4200156, at *8-11 (N.D.Ga. Apr. 21, 2008); United States v. Madison, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012). A minority of courts reached the opposite conclusion. See, e.g., In re Application of the United States, 809 F.Supp.2d 113 (E.D.N.Y. 2011); In re Application of the United States, 747 F.Supp.2d 827 (S.D.Tex. 2010); In re Application of the United States 733 F.Supp.2d 939,943 (N.D. Ill. 2009); United States v. Forest, 355 F.3d 942 (6th Cir. 2004) *judgment vacated on other grounds sub. nom. Garner v. United States*, 543 U.S. 1100 (2005). There has been a similar split of opinion among Massachusetts Superior Court judges. *Compare*, Commonwealth v. Pitt, 2012 WL 927095, at *1 (Mass. Super. Feb. 23, 2012), *with*, Commonwealth v. Tewolde, Suffolk Superior Court No. 11-10677 (2012)

and Commonwealth v. Williams, Suffolk Superior Court No. 2009-10960 (2013). With these conflicting opinions as the backdrop, this Court is in the difficult position of having to predict what the SJC might do if presented with this issue. That in turn requires some understanding as to the direction that the United State Supreme Court has taken, since its Fourth Amendment analysis clearly informs any outcome under article 14.

From the 1960s until the Supreme Court's most recent decision in United States v. Jones, 132 S.Ct. 945 (2012), the test for determining whether a search has occurred under the Fourth Amendment has been that first articulated in Justice Harlan's concurring opinion in Katz v. United States, 389 U.S. 347, 361 (1967). Agreeing with the majority that the Fourth Amendment "protects people, not places," Justice Harlan stated that the rule emerging from prior decisions of the Court embraced a two fold requirement—first, that one "have exhibited an actual (subjective) expectation of privacy" and second, that "the expectation be one that society is prepared to recognize as reasonable." 389 U.S. at 361. The SJC has adopted the same test for article 14 purposes. Commonwealth v. Podgurski, 386 Mass. 385 (1982).

In adopting the reasonable expectation of privacy test, the Supreme Court moved beyond more traditional property-based notions of what constituted a search under the Fourth Amendment. Indeed, in holding that federal agents in Katz had engaged in a "search" by listening in on a telephone conversation of the defendant with a device attached to the outside of a telephone booth, Justice Stewart, writing for the majority, scoffed at the government's argument that there could be no Fourth Amendment violation because there was no physical intrusion into the booth itself: because the Fourth Amendment protects people and not simply

physical spaces, the presence or absence of a trespass was not determinative. Although the Katz decision was hailed as a watershed in Fourth Amendment jurisprudence, the test that it established, precisely because it is so abstract, has proved difficult to apply. This is especially true as to technology developed in the last two decades which allows for electronic monitoring of an individual's movements.

The first Supreme Court case to address location surveillance was United States v. Knotts, 460 U.S. 276 (1983), involving the police installation of a beeper into a drum which was then loaded onto the defendant's car. The Court there held that a "person traveling in an automobile on public thoroughfares has no expectation of privacy in his movements from one place to another." 460 U.S. at 281. The beeper was simply a "scientific enhancement" which allowed police to conduct visual surveillance more easily. The Court reached a different result, however, in United States v. Karo, 468 U.S. 705 (1984), where a beeper was installed in drums of ether that were moved into a private residence and storage lockers. The beeper's location inside the house was then used to secure a search warrant for the residence. "We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine, by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time." Id. at 715-716.

Then came the Supreme Court's decision in United States v. Jones. In that case, government agents attached a GPS tracking device to a car used by the defendant and subsequently tracked his movement for the next 28 days. A unanimous Court held that the

government's action violated the Fourth Amendment, but the justices were divided as to how they reached that result. Writing for the majority, Justice Scalia (joined in his opinion by Thomas, Kennedy and Roberts) focused on the fact that the GPS device was attached to a car and thus physically intruded on private property even as the car itself traveled on public roads. Although acknowledging that Katz moved away from a strictly property-based approach, Scalia wrote that it was not meant to supplant the more traditional prohibition against trespass by governmental officials. Because the case before the Court could be decided based on the fact that the federal agents engaged in a trespass, Scalia (and those who joined him) concluded that the Court need go not further in its analysis.

Five justices, however, were not content to leave it at that. Justice Alito, joined by Justices Breyer, Kagan and Ginsburg, wrote a concurring opinion critical of Scalia's emphasis on common-law trespass, labeling it a return to "18th century tort law." 132 S.Ct. at 957. Alito and those justices who joined him were of the view that it did little to address those situations certain to arise in the future where there is tracking without any physical intrusion. The Alito opinion noted in particular the technology relating to cell phones and other wireless devices which now permits wireless carriers to track and record locations of users. In an earlier pre-computer time, law enforcement surveillance was constrained by the impracticality of constant monitoring, which would have required a large team of agents, multiple vehicles and perhaps aerial assistance. Now, with this technology installed in many smart phones, such surveillance is easy and cheap. 132 S. Ct. at 963.

Justice Sotomayor joined in Scalia's opinion only because she was willing to accept his position that Katz did not supplant entirely a test focused on a trespass. She wrote separately, however, to emphasize that GPS monitoring of one's movements also constitutes an abridgement of one's reasonable expectation of privacy. Although an individual's movements may be on public byways, tracking those movements nevertheless presents the potential of allowing government to generate "a precise, comprehensive record" of a person's private life that reflects a "wealth of detail about her familial, political, professional, religious and sexual associations." 132 S.Ct. at 955. Sotomayor agreed with Alito that this kind of high-tech monitoring is cheap in comparison with conventional surveillance techniques and, because it is carried out surreptitiously, "evades the ordinary checks that constrain invasive law enforcement practices: 'limited police resources and community hostility.'" 132 S.Ct. at 956, quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004). She also took on the notion that, because digital information is typically shared with third parties, this somehow means that the information loses its constitutional protection. People regularly disclose intimate details about their personal lives to online retailers, for example, without any expectation that such information can be mined by the government.

Although United States v. Jones may have unsettled the legal landscape in some states, the SJC had already held under article 14 that the government's attachment of a GPS device to a vehicle in order to monitor a suspect's movements required a warrant supported by probable cause. Commonwealth v. Connolly, 454 Mass. 808, 818 (2009). Like the Supreme Court, the justices in Connolly split as to how they reached that conclusion. Writing for the majority, Justice Cowin focused on the fact that, to install the device, police not only had to enter into the

car but also relied on the vehicle's electrical system to power it—an ongoing physical intrusion. "It is a seizure not by virtue of the technology employed but because the police use private property (the vehicle) to obtain information for their own purposes." 454 Mass. at 823. Three justices disagreed with that property-based approach: in a concurring opinion in which Justices Botsford and Cordy joined, Justice Gants wrote that "the appropriate constitutional concern is not the protection of property but rather the protection of the reasonable expectation of privacy." 454 Mass. at 833. Quoting a New York Court of Appeals decision, he pointed out that GPS technology permits the government to put together "a highly detailed profile, not simply of where we go, but by easy inference of our associations—political religious, amicable and amorous—to name only a few..." 454 Mass. at 834, quoting People v. Weaver, 12 N.Y.3d 433, 441-442 (2009). That ability to put together a mosaic of one's personal life is precisely what concerned five justices of the Supreme Court.

Turning to the instant case, this Court must decide if CSLI is somehow different than GPS monitoring such that the SJC, if it were to address the issue, would likely reach a result different than it did in Connolly. The government argues that CSLI is different, for several reasons. First, the Commonwealth suggests that because CSLI does not involve the placement of any tracking device on private property, there is no constitutional violation. Particularly in light of the concurring opinions in Jones, this Court does not believe that the SJC today will confine its article 14 analysis to trespass and property-based notions. Second, the Commonwealth argues that CSLI is far less precise in determining an individual's location than a GPS device is, since it gives only the location of the cell tower, not the cell phone user. In order to take this argument seriously, however, 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). Finally, the Commonwealth contends that the cell phone user has no reasonable expectation of privacy in CSLI because he or she has voluntarily transmitted the information to the cell phone provider. This argument requires more discussion, since this reliance on the so-called "third party doctrine" is the foundation for many lower court decisions holding that government access to CSLI does not implicate the Fourth Amendment. See e.g. United States v. Graham, 846 F.Supp.2d 384, 397 (D.Md. 2012); see also Commonwealth v. Williams, Suffolk Superior Court No. 2009-10960 (2013).

The third party doctrine stems from two cases, both of which predate the digital age. The first was United States v. Miller, 425 U.S. 435 (1976), where federal agents subpoenaed the defendant's bank records to show that he had written checks to buy equipment used to distill black market whiskey. The Court held that the records were not the defendant's private papers but rather the business records of the bank, pertaining to transactions to which the bank itself was a party. Id. at 440-441. The second case was Smith v. Maryland, 442, U.S. 735 (1979), which concerned government installation of a "pen register" that allowed it to collect the telephone numbers dialed from the petitioner's home. In holding that there was no intrusion into the petitioner's reasonable expectation of privacy, the Supreme Court reasoned that people understand that when they dial a number, they are conveying that information to the telephone company. They also know that a record is kept of that information since (at least with respect to long distance calls) the numbers are reflected on their telephone bills. Relying on Miller, the Court went on to hold that any subjective expectation of privacy would not be reasonable in any

event: by voluntarily conveying numerical information to the telephone company, the petitioner "assumed the risk" that the company would reveal to police the numbers that he dialed.

Simply stating the facts of these two cases shows just how inapt they are when one applies them to CSLI. The ordinary cell phone user may understand that radio waves are sent out to connect his calls, but 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. More significant, 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 receiving or making a call. Finally, 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. In 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.

The Commonwealth's final argument is that, because this case involves access to CSLI for a limited period of time, it is entirely different from the longer-term "real time" monitoring at issue in United States v. Jones. The first part of this argument—that the CSLI is historical or backward looking and therefore somehow less intrusive than real time monitoring—is unpersuasive. The temporal difference between prospective and historic location tracking has no bearing on whether one has any reasonable expectation of privacy in that information. See e.g. In re Application of the United States for an Order Authorizing the Release of historical Cell-Site Data, 747 F.Supp.2d 827, 839 (S.D. Tex. 2010). The Commonwealth is on stronger grounds

when it contends that government monitoring of a suspect's movement for a limited period of time does not implicate the concerns voiced by at least five justices in United States v. Jones. Those five (Alito, Sotomayor, Kagan, Breyer, and Ginsburg) appeared to endorse the reasoning of the D.C. Circuit Court decision that was under review in Jones, United States v. Maynard, 615 F.3d. 544 (D.C. Cir. 2012).

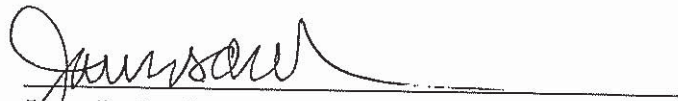
In Maynard, the Court emphasized the prolonged nature of the surveillance (there 28 days), with the sequence and repetition of a person's movements revealing much more than the tracking of that same person on a single day. "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person but all such facts." 615 F.3d 562. Justice Alito appeared to endorse this approach in Jones when he suggested that it was the long-term nature of the GPS monitoring which impinges on expectations of privacy. "We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark." 132 S.Ct. at 964. The problem with this approach is itself suggested by Alito's statement—where does one draw the line?

Certainly, one way to answer this question in the instant case is precisely as Alito did: without stating where the line is, this Court could conclude that 14 days of CSLI is sufficiently prolonged to implicate article 14. A more satisfactory answer, however, 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 never have been able to obtain by standard

police surveillance techniques. This is particularly true where the CSLI is historical since it allows 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 government to access this information is clearly a good thing. However, without that minimal limit on governmental power, all of us (at least those of us with cell phones) are at risk.

CONCLUSION AND ORDER

For all the foregoing reasons, the defendant's Motion to Suppress Evidence is
ALLOWED.



Janet L. Sanders
Justice of the Superior Court

Dated; April 2, 2013