

---

---

**Commonwealth of Massachusetts  
Supreme Judicial Court**

**SJC-13144**

---

**Commonwealth  
Appellee**

**v.**

**Jerron Perry  
Appellant**

---

**Interlocutory Appeal From an Order of the  
Suffolk Superior Court**

---

**BRIEF FOR APPELLANT, JERRON PERRY**

ERIC TENNEN, BBO # 650542  
Swomley and Tennen, LLP  
50 Congress St. #600  
Boston, MA 02109  
(617) 227-9443

August, 2021

---

---

**TABLE OF CONTENTS**

Table of Contents . . . . . 2

Table of Authorities . . . . . 4

Issue Presented . . . . . 9

Statement of the Case . . . . . 9

Statement of Facts . . . . .10

Summary of the Argument . . . . .16

Argument . . . . . 18

**I. Perry had a subjective expectation of privacy in his CSLI, and there was no dispute his telephone was part of the tower dump data . . . . . 20**

**II. Any warrant for the CSLI of an unspecified individual or telephone number—especially when it seeks the data of 50,951 innocent persons—is an unconstitutional general warrant. . . . . 22**

*A. The (State and Federal) Framers designed the Constitutions to eliminate general warrants by requiring particularity and probable cause. . . . .22*

*B. The Constitutions have adapted to new technologies. . . . .25*

*C. A warrant seeking the CSLI for an identified individual and identified phone number is not a “general warrant” . . . . .27*

*D. Neither the “safe harbor” rule, nor the mosaic theory plays a role in this case. . . . .30*

*E. Orders authorizing searches of an unspecified number of persons and/or phone numbers are general warrants. . . . .34*

i. Warrants that knowingly sweep up countless innocent persons lack particularity. . . . . . 40

ii. Without information that a phone had been used during the crimes, the affidavit did not provide the requisite nexus to establish probable cause nor “reasonable belief” under § 2703(d). . . . . . 43

Conclusion . . . . . 49

Addendum . . . . . 50

Certificate of Service . . . . . 67

Certificate of Compliance . . . . .67

## TABLE OF AUTHORITIES

### Cases

<i>Carpenter v. U.S.</i> , 138 S.Ct. 2206 (2018) . . . . .	26, 30, 38
<i>Commonwealth v. Almonor</i> , 482 Mass. 35 (2019) . . . . .	43
<i>Commonwealth v. Amaral</i> , 398 Mass. 98 (1986) . . . . .	35
<i>Commonwealth v. Amato</i> , 80 Mass. App. Ct. 230 (2011) . . . . .	36
<i>Commonwealth v. Anthony</i> , 451 Mass. 59 (2008) . . . . .	45
<i>Commonwealth v. Augustine</i> , 467 Mass. 230 (2014) . . . . .	<i>passim</i>
<i>Commonwealth v. Augustine</i> , 472 Mass. 448 (2015) . . . . .	<i>passim</i>
<i>Commonwealth v. Cundriff</i> , 382 Mass 137 (1980) . . . . .	23
<i>Commonwealth v. Dorelas</i> , 473 Mass. 496 (2016) . . . . .	25
<i>Commonwealth v. Estabrook</i> , 472 Mass. 852 (2015) . . . . .	27, 28, 29
<i>Commonwealth v. Erickson</i> , 14 Mass. App. Ct. 501 (1982) . . . . .	24, 41

<i>Commonwealth v. Fulgiam,</i> 477 Mass. 20 (2017) . . . . .	21
<i>Commonwealth v. Henley,</i> (SJC-12951 August 5, 2021) . . . . .	32, 47, 48
<i>Commonwealth v. Hobbs,</i> 482 Mass. 538 (2019) . . . . .	29, 43
<i>Commonwealth v. Holley,</i> 478 Mass. 508 (2017) . . . . .	24, 25
<i>Commonwealth v. Jordan,</i> 91 Mass. App. Ct. 743 (2017) . . . . .	29, 44
<i>Commonwealth v. Kaupp,</i> 453 Mass. 102 (2009) . . . . .	25
<i>Commonwealth v. Lett,</i> 393 Mass 141 (1984) . . . . .	22
<i>Commonwealth v. Louis,</i> 487 Mass. 759 (2021) . . . . .	46
<i>Commonwealth v. Matias,</i> 440 Mass. 787 (2004) . . . . .	44
<i>Commonwealth v. McCarthy,</i> 484 Mass. 493 (2020) . . . . .	26, 27, 36, 37
<i>Commonwealth v. Mora,</i> 485 Mass. 360 (2020) . . . . .	18, 32
<i>Commonwealth v. Morin,</i> 478 Mass. 415 (2017) . . . . .	24, 46
<i>Commonwealth v. Perkins,</i> 478 Mass. 97 (2017) . . . . .	24

<i>Commonwealth v. Smith</i> , 370 Mass. 335 (1976) . . . . .	24, 41
<i>Commonwealth v. Snow</i> , 486 Mass. 582 (2021) . . . . .	44, 46
<i>Commonwealth v. Vasquez</i> , 482 Mass. 850 (2019) . . . . .	45
<i>Commonwealth v. White</i> , 475 Mass. 583 (2016) . . . . .	45, 46
<i>Commonwealth v. Wilkerson</i> , 486 Mass. 159 (2020) . . . . .	22, 29
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971) . . . . .	23
<i>Illinois v. Lidster</i> , 540 U.S. 419 (2004) . . . . .	26
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001) . . . . .	26
<i>Leaders of a Beautiful Struggle v. Baltimore Police Department</i> , 2 F.4th 330 (4 <sup>th</sup> Cir. 2021) . . . . .	39
<i>Matter of Search of Information Stored at Premises Controlled by Google</i> , 481 F.Supp.3d 730 (N.D. Ill 2020) . . . . .	18, 41, 45
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965) . . . . .	23, 24
<i>State v. Earls</i> , 214 N.J. 564 (2013) . . . . .	43

<i>U.S. v. Christine</i> , 687 F.2d 749 (3d Cir. 1982) . . . . .	22
<i>U.S. v. Jones</i> , 565 U.S. 400 (2012) . . . . .	37

**Statutes/Rules**

U.S. Constitution, Amendment IV . . . . .	<i>passim</i>
Mass. Declaration of Rights, Article XIV . . . . .	<i>passim</i>
18 U.S.C. § 2703. . . . .	<i>passim</i>
M.G.L. c. 66A, § 2 . . . . .	36
Mass. R. Crim. P. 13(a)(2) . . . . .	20

**Other Sources**

Elizabeth Tsai Bishop, <i>et al.</i> , Harvard Law School, Criminal Justice Policy Program, <i>Racial Disparities in the Massachusetts Court System</i> , (2020) . . . . .	39
Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 26 (2012). . . . .	32

## INTRODUCTION

Imagine you were walking down the street and the police stopped you and said: “We are conducting an investigation and want to record that you were here, at this location, on this day, by getting your phone number. Is that ok?” Some people might say yes, some might not. Imagine now that the police say, “we are conducting an investigation from months ago and want to see if you were here then—is that ok?” Some might say yes, more would not. Now imagine the police never spoke to you—rather, you find out that they tracked your location, through your cell phone, at various times months ago, while you were conducting personal business. They also know the phone numbers of who you called/texted (or who called/texted you) and still have your data. They did not ask for your consent and there is nothing you can do about it. Not only did the police do this to you, they do this to 50,951 people. How many people would be ok with that? Very few, if any. That is the privacy intrusion at issue in this case.



## **ISSUES PRESENTED**

1. In his motion to suppress, Perry made a “four corners” challenge to the search warrants. Perry submitted an affidavit stating he did not consent to the search. Additionally, the government’s evidence established that Perry’s phone was one of the numbers searched in the tower dump. Consequently, did Perry have standing to contest the warrants?
  
2. During a criminal investigation, law enforcement had no suspects. They did not even have information about whether the culprit(s) used a cell phone at any point during the crimes. Despite that, law enforcement sought a warrant for cell site location information (“CSLI”) —not of an identified individual nor a single phone but, rather, of every phone number in the vicinity of the crimes. Did law enforcement obtain, and execute, an unconstitutional general warrant lacking particularity?
  
3. In its warrant affidavit, the government agent admitted he had no information a cell phone was used during the commission of these crimes. Rather, he assumed it was because cell phones are so ubiquitous. Did law enforcement obtain, and execute, an unconstitutional general warrant lacking the requisite nexus to establish probable cause or “reasonable belief” under § 2703(d)?

## **STATEMENT OF THE CASE**

Perry was indicted in October 2019 on various serious charges, including one count of first-degree murder, multiple counts of masked armed robbery, and related

firearm offenses.<sup>1</sup> *See* R.A. Vol 1, pg. 12. He filed a motion to suppress evidence obtained from various warrants in September 2020. After multiple stages of briefing, a Superior Court judge denied the motion on April 21, 2021. *See* Addendum. Perry filed a timely notice of interlocutory appeal; a single justice of this Court allowed the motion on July 2, 2021 and referred it to the full bench. *See* SJ-2021-0211. In his order, he asked the parties address, *inter alia*, “the premise that most individuals use cellular telephones and keep them turned on, in connection with the issue of probable cause to obtain the search warrant.” *Id.*

## **STATEMENT OF THE FACTS**

### A. The Warrants

The factual background is largely undisputed and summarized succinctly by the motion judge. In Fall, 2018, authorities were investigating a series of armed robberies, one of which resulted in a shooting death. Having no

---

<sup>1</sup> Perry was later indicted for related charges in Norfolk Superior Court. Those matters were transferred to Suffolk Superior Court and both cases are proceeding together.

specific suspect, agents sought broad search warrants: 1) the October 26, 2018 warrant for cell site location information (“CSLI”) for 15-minute periods before and after four specific dates corresponding with four of the incidents and 2) the January 30, 2019 warrant for CSLI for 40-minute periods before and after three different dates corresponding with three other incidents. *See* Motion Judge’s Order, pg. 2 (Addendum). The authorities sought data for seven dates, though later determined that one of them was unrelated to this investigation. *Ibid.* Additionally, “[f]or each communication that had occurred during that time period, including those that began before or ended after that period, the warrant also sought source and destination telephone numbers; date time, and duration of the communication; sector (face of the tower); and type of communication, e.g., text, phone call.” *Ibid.*

The authorities did not have a suspect. Importantly, they could not say if a cell phone was used:

While the FBI cannot state definitively that the Suspect possessed a cellular telephone during

the commission of the Target Offenses, and if so, what cell numbers(s) he possessed at that time, based on my training and experience, it is very common for a person to have a cellular telephone with them at all times, even during and after the commission of a crime. As part of its investigation, the FBI is also attempting to determine the existence and identity of any individuals and/or co-conspirators, such as the drivers of the vehicles, who may have assisted the Suspect in the commission of the Target Offenses.

R.A. Vol 2, pg. 21. The most they could say is that they believed the suspect worked with a co-conspirator and that “co-conspirators will contact each other via phone if they are separated prior to, an/or during, and/or immediately after the actual commission of a violent crime.” R.A. Vol. 2, pg. 45.

From these two warrants alone, the authorities obtained information from 50,951 unique phone numbers. R.A. vol. 2, pg. 50 (thumb drive). The October warrant produced data for 14,121 unique numbers; the January warrant produced data for another 36,830 unique numbers. *Ibid.* That total number does not include duplicates. The October warrant produced additional data for 15,926

duplicate numbers; the January warrant produced additional data for 59,002 duplicate numbers. *Ibid.*

After the warrants issued, the police received the requested information and they were eventually able to identify phone numbers which they linked to Perry and his co-defendant. *See* Motion Judge's Order, pg. 3-4 (Addendum).

Based on the fruits of these initial warrants, the Commonwealth obtained multiple additional search warrants for, *inter alia*, the suspects' phones, homes, cars, and Google histories. Following execution of all these warrants, Perry was ultimately indicted.

#### B. The Judge's Order

The Motion Judge agreed Perry had standing to contest the search. First, he held that counsel's affidavit satisfied Mass. R. Crim. P. 13(a)(2). *See* Motion Judge's Order, pg. 4 (Addendum); R.A. Vol. 1, pg 29. Second, citing *Commonwealth v. Augustine*, 467 Mass. 230. 255 (2014), he

noted “that one has a reasonable expectation of privacy in one’s cell phone location.” *Id.*

As to the merits, he summarized the affiant’s attempt at establishing probable cause:

The affidavits supporting the warrant applications do not identify a suspect by name. Nor do they include any evidence that the perpetrator or perpetrators used a cell phone during the relevant time periods. Probable cause is based on the fact that (1) almost everyone has a cell phone and carries it with them; (2) most cell phones record one’s whereabouts, even when not being actively used; (3) based on similarities between the offenses as set forth in the affidavits, it is likely that the same person committed all six crimes, possibly with one or more co-venturers; and (4) it is therefore likely that the same cell phone was in the vicinity of several or all of the six incidents.

*Id.* at 3. He concluded this was enough:

Implicit in the showing of probable cause in this context is the unlikelihood that someone *not* involved in the robberies and attempted robbery would happen to have been close to the scene of two or more crimes that occurred in Boston and Canton or different parts of Boston. The Court credits statements in the supporting affidavits from experienced law enforcement officers that most people use cell phones and keep them on. Therefore, there was a “substantial basis”, see *White*, 475 Mass. at 588, to conclude that the historical CSU obtained through these searches

would identify one or more common denominator cell phone numbers, *i.e.* numbers for cell phones that were in the vicinity of two or more crimes that occurred in different areas.

*Id.* at 6-7.

He then held the warrants were not “overbroad, unparticularized general warrants.” He listed five reasons supporting this conclusion:

*First*, although the intrusion was surreptitious to anyone unaware of how CSLI is collected, it did not involve intruding into any non-public space. Moreover, most cell phone users are aware at least to some extent that their locations are conveyed to cell phone providers in order to receive cell phone service.

*Second*, the nature of the information collected here was non-invasive, consisting of historical CLSI [sic] and phone numbers, not names or other personal identifying information, and the type of communication (e.g. text, cell phone), not the content of any communication. While users’ locations were identified, they were anonymous with no or limited tracking of movement.

*Third*, the searches were extremely limited temporally, involving only 15 minutes or 40 minutes of time. This was the opposite of a “mosaic,” in which limited surveillance is aggregated to reveal a complex picture of an individual life.

*Fourth*, law enforcement officers provided detailed affidavits explaining a nexus to criminality and why the sought information would be useful in identifying one or more suspects.

*Fifth*, although the warrants were broad in the sense of capturing extensive information that federal agents and detectives knew would not be needed for further investigation. they were not *overbroad* because there was no less intrusive way to identify the suspects in the crimes under investigation, *i.e.* a string of robberies and an attempted robbery that led to a fatal shooting. Without the name or phone number of a suspect law enforcement officers did not know which of the four cell phone companies provided cell phone service to any suspect who had a cell phone. Moreover, as noted above, all of the locations and timeframes were closely targeted to the scene and time of the crimes.

*Id.* at 8-10 (citations omitted).

### **SUMMARY OF THE ARGUMENT**

As someone whose phone number was targeted by the Commonwealth, Perry has standing to contest the warrants. He brought a “four corners” motion, the Commonwealth knew his phone number was included in the tower dump, and his affidavit established he did not consent to these searches.



The Federal and State constitutions prohibit general warrants by, *inter alia*, requiring particularity and probable cause. Even as technology evolves, this Court has adopted these requirements to the issue at hand. With respect to CSLI data, this Court has allowed warrants *if* there is an identified suspect, and identified phone number, and a nexus between the crime and the fact a phone was used. This Court has only made an exception if the Commonwealth is seeking six (or less) continuous hours of data. But in those so-called “safe harbor” cases, the Commonwealth still needs to satisfy the requirements of 18 U.S.C. § 2703.

This Court has never approved of warrants that seek CSLI data of anyone in the vicinity of the crime when the Commonwealth lacked a suspect, phone number, and information that a phone was even used. Warrants that broad implicate a host of privacy related issues and are plainly general warrants.

These general warrants lack particularity because they do not specify a person or place to be searched, much like unconstitutional “all person” warrants. They also lack probable cause and do not comply with 18 U.S.C. § 2703 because there is no information that a phone was used during the commission of the crime. A warrant lacking either requirement is an unconstitutional general warrant.

## **ARGUMENT**

### **Standard of Review**

“Because the judge’s findings were based entirely on documentary evidence, [this Court] review[s] both his findings of fact and his conclusions of law de novo.”

*Commonwealth v. Mora*, 485 Mass. 360, 364 (2020).

### **Argument Introduction**

This case presents an issue of first impression: whether, when the Commonwealth obtains a cell tower dump warrant<sup>2</sup> for every individual at a certain place and

---

<sup>2</sup> The Superior Court judge referred to this as “cell tower dump or other ‘geofence’ warrants.” The terms are often used interchangeably. *See e.g. Matter of Search of*

time, in the absence of a specific suspect or information that the suspect used a phone, it does so in violation of the Federal and Massachusetts Constitutions.

The Court below authorized the Commonwealth’s approach of obtaining a haystack in hopes of finding a needle. What the Commonwealth did here was nothing like what this Court has sanctioned under *Commonwealth v. Augustine*, and progeny. It was an unconstitutional overreach that gravely threatens the privacy of every person.

---

*Information Stored at Premises Controlled by Google*, 481 F.Supp.3d 730 (N.D. Ill 2020). The individual information contained in the cell tower dumps is referred to as “telephone call cell site location information.” See *Commonwealth v. Augustine*, 467 Mass. 230, 259 (2014) (Gants, C.J. dissenting). That “provides the approximate physical location (location points) of a cellular telephone only when a telephone call is made or received by that telephone.” *Id.* Telecommunications companies can also sometimes provide “registration CSLI” which is “the approximate physical location of a cellular telephone every seven seconds unless the telephone is ‘powered off,’ regardless of whether any telephone call is made to or from the telephone.” *Id.* At issue here is the former—telephone CSLI obtained from a cell tower dump warrant.

**I. Perry had a subjective expectation of privacy in his CSLI, and there was no dispute his telephone was part of the tower dump data.**

The Commonwealth may argue that Perry does not have standing to contest the search. That argument is meritless. Counsel submitted an affidavit and memorandum making clear this was a “four corners” motion and that Perry had never consented to the search. R.A. Vol 1, 29. Additionally, the Commonwealth’s own evidence (which included the warrant affidavits, a prior motor vehicle stop, and an interrogation) confirmed Perry’s phone number and that it was included in the tower dump. This was enough to give Perry standing. The motion judge agreed. *See* Motion Judge’s Order (Addendum)

First, the purpose of the affidavit requirement of Rule 13(a)(2) is to put the court and the Commonwealth on notice of the facts that will be used to support the motion (at a hearing). Between counsel’s affidavit and the motion itself, the Commonwealth (and Judge) were clearly on notice as to the nature of the argument.

Second, individuals have an expectation of privacy in the CSLI and other private data associated with their phones. To establish standing, it is enough that the Commonwealth confirms a phone number among the CSLI data belongs to the defendant. *See Commonwealth v. Fulgiam*, 477 Mass. 20, 33-34 (2017) (defendant “provided the police with his cellular telephone number prior to his arrest. At trial he offered the CSLI associated with the cellular telephone account as evidence ...implicitly claiming ownership of the cellular telephone account; and the cellular telephone associated with the [ ] number was seized from [defendant] pursuant to a search warrant prior to his arrest. Moreover, the Commonwealth consistently attributed the cellular telephone account to Corbin”); *Commonwealth v. Augustine*, 467 Mass. 230, 254-55, n. 38 (2014). The information available to the Commonwealth, and motion judge, clearly established Perry’s standing.

Given that 50,951 people were tracked through their phones, it would be outrageous to say no one had standing

to challenge the search. It would authorize the Commonwealth to seek these records with impunity, knowing no one—not even someone they ultimately charge—could challenge their actions.

**II. Any warrant for the CSLI of an unspecified individual or telephone number—especially when it seeks the data of 50,951 innocent persons—is an unconstitutional general warrant.**

*A. The (State and Federal) Framers designed the Constitutions to eliminate general warrants by requiring particularity and probable cause.*

A warrant either is, or is not, a general warrant. If it is, there is no middle ground—it is unconstitutional. *See Commonwealth v. Wilkerson*, 486 Mass. 159, 168-69 (2020). Accordingly, “*all* evidence seized pursuant to a *general* warrant must be suppressed.” *Commonwealth v. Lett*, 393 Mass 141, 145-146 (1984), *quoting U.S. v. Christine*, 687 F.2d 749, 758 (3d Cir. 1982) (emphasis in original). That’s because “[t]he cost to society of sanctioning the use of general warrants—abhorrence for which gave birth to the Fourth Amendment—is intolerable by any

measure. No criminal case exists even suggesting the contrary.” *Ibid.*

So, what is a general warrant? Typically, a “general warrant” refers to a warrant that allows the government to rummage freely through an individual’s belongings. *See Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

In Tudor England, officers of the Crown were given roving commissions to search where they pleased in order to suppress and destroy the literature of dissent, both Catholic and Puritan. In later years, warrants were sometimes more specific in content, but they typically authorized of all persons connected of the premises of all persons connected with the publication of a particular libel, or the arrest and seizure of all the papers of a named person thought to be connected with a libel.

*Stanford v. Texas*, 379 U.S. 476, 482-83 (1965). The writs of assistance were a kind of general warrant “which allowed officers of the crown to search, at their will, wherever they suspected untaxed goods to be, and granted the officials the right of forcible entry.” *Commonwealth v. Cundriff*, 382 Mass 137, 143 (1980). To eliminate general warrants, the Federal and Massachusetts Constitutions codified, *inter*

*alia*, the need for particularity and probable cause. *See* U.S. Const. Amd. IV; Article XIV, Mass. Decl. of Rights; *Stanford*, 379 U.S. at 481; *Commonwealth v. Morin*, 478 Mass. 415, 425 (2017).

Particularity “makes general searches under them impossible,” and “[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” *Stanford*, at 485. Thus, a warrant must describe “with particularity the places to be searched and the items to be seized.” *Commonwealth v. Holley*, 478 Mass. 508, 524 (2017), quoting *Commonwealth v. Perkins*, 478 Mass. 97, 106 (2017). Particularity protects against general searches of all kinds. It prevents broad “all person” warrants which “risk that an innocent person may be swept up in a dragnet and searched.” *Commonwealth v. Smith*, 370 Mass. 335, 346 (1976). Likewise, it prohibits indiscriminate searches of entire buildings when only one unit is targeted. *See Commonwealth v. Erickson*, 14 Mass. App. Ct. 501, 504 (1982). It even restricts the government from searching



through all the files in a phone when there is only probable cause to search some. *See Commonwealth v. Dorelas*, 473 Mass. 496, 502 (2016).

The Constitutions also require “probable cause.” Probable cause exists when there is a “‘substantial basis’ to conclude that ‘the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues.’” *Holley*, at 521 *quoting Commonwealth v. Kaupp*, 453 Mass. 102, 110 (2009). “In other words, the government must show not only that there is probable cause that the individual committed a crime but also that there is a ‘nexus’ between the alleged crime and the article to be seized.” *Commonwealth v. Snow*, 486 Mass. 582, 586 (2021).

*B. The Constitutions have adapted to new technologies.*

The constitutional disdain for general warrants met the moment in the colonial era. As the world evolved, Courts “assure[d] preservation of that degree of privacy

against government that existed when the Fourth Amendment was adopted.” *Carpenter v. U.S.*, 138 S.Ct. 2206, 2214 (2018) quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001). New technology meant a more watchful eye:

The surveillance implications of new technologies must be scrutinized carefully, lest scientific advances give police surveillance powers akin to these general warrants. Just as police are not permitted to rummage unrestrained through one’s home, so too constitutional safeguards prevent warrantless rummaging through the complex digital trails and location records created merely by participating in modern society.

*Commonwealth v. McCarthy*, 484 Mass. 493, 498-99 (2020) (citations omitted).

Colonial general warrants were at least subject to the practical constraints posed by “limited police resources and community hostility.” *Illinois v. Lidster*, 540 U.S. 419, 426 (2004). On the other hand, “advancing technology undercuts traditional checks on an overly pervasive police presence because it (1) is not limited by the same practical constraints that heretofore effectively have limited long-running surveillance, (2) proceeds surreptitiously, and (3)

gives police access to categories of information previously unknowable.” *McCarthy*, 484 Mass at 499.

*C. A warrant seeking the CSLI for an identified individual and identified phone number is not a “general warrant.”*

The framers eradicated general warrants and courts assured those protections apply even as surveillance techniques evolve. When it became possible to seek CSLI, this Court set parameters to assure the government did not cross the constitutional line.

The government must always get a warrant, particular and supported by probable cause, to obtain any iota of registration CSLI. *See Commonwealth v. Estabrook*, 472 Mass. 852, 858 n.12 (2015). To get more than six-hours of telephone CSLI, the Commonwealth must also obtain a warrant, particular and supported by probable cause. *Ibid.* If, however, the Commonwealth is seeking less than six hours of telephone CSLI, it does not need a “probable cause” warrant; but in these so called “safe harbor” cases, it must

still comply with the requirements of 18 U.S.C. § 2703.<sup>3</sup> *Augustine* at 266 (Gants, J., dissenting); *Estabrook*, at 858. Compliance with § 2703(d), in turn, requires “a showing of ‘specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.’” *Augustine* at 266-67 (Gants, J., dissenting) (citations omitted); 18 U.S.C. § 2703(d).

To summarize, obtaining any kind of CSLI data requires a warrant. Each warrant must still be particular. Warrants for registration CSLI, or six-plus hours of telephone CSLI, require probable cause; § 2703(d) warrants for less than six hours of telephone CSLI require, essentially, reasonable suspicion.

---

<sup>3</sup> 18 U.S.C. § 2703(a) refers to these orders as “warrants.” This brief will refer to them as “§ 2703(d) warrants,” as opposed to “probable cause” warrants issued in the more traditional course.

This Court explained these parameters amidst a backdrop of extremely important factors. Every case dealing with requests for telephone (or registration) CSLI was for an “identified” suspect and specific phone number. *See e.g. Commonwealth v. Wilkerson*, 486 Mass. 159 (2020); *Commonwealth v. Hobbs*, 482 Mass. 538, 544 (2019); *Commonwealth v. Augustine*, 472 Mass. 448 (2015); *Commonwealth v. Jordan*, 91 Mass. App. Ct. 743 (2017). Even in cases of “safe harbor” orders, this Court was clear: a § 2703(d) order was only enough to obtain the data of an “identified person’s cellular telephone.” *See e.g. Commonwealth v. Estabrook*, 472 Mass. 852, 858 (2015).

And even though this Court allowed for a six-hour “safe harbor” where it did not require a *probable cause* warrant, it did so because the Commonwealth would still need to obtain a § 2703(d) warrant. It went without saying that absent compliance with the minimal requirements of § 2703(d), any order for telephone CLSI would simply be a general warrant—seeking data of unspecified persons or

telephone numbers. Essentially, it would be warrant permitting the government to “rummage” through phone records of innocent persons hoping to find something incriminating.

*D. Neither the “safe harbor” rule, nor the mosaic theory, plays a role in this case.*

It is important to pause here and reflect on this Court’s “safe harbor” rule because the Commonwealth may argue it is implicated in this case. The rule arose prior to the U.S. Supreme Court’s decision in *Carpenter v. U.S.*, 138 S.Ct. 2206 (2018). The *Carpenter* court held plainly that “when the Government accessed CSLI from the wireless carriers, it invaded Carpenter’s reasonable expectation of privacy in the whole of his physical movements.” *Id.* at 2219. The Court did not decide if there was a “limited period for which the Government may obtain an individual’s historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be.” *Id.* at 2217, n. 3. It is not clear if this Court’s “safe harbor” rule thus survived

*Carpenter*. Nevertheless, the facts of this case do not require this Court to revisit that rule now.

Even under the “safe harbor” rule, the Commonwealth must still comply with the requirements of § 2703(d); as argued below, it did not do so here. More importantly, in holding that an individual did not have an expectation of privacy in less than six hours of CSLI data, this Court could only have been referring to six continuous hours. Though the total time of data sought here was less than six cumulative hours, it came from data spanning six days over the course of five weeks. Six consecutive hours of CSLI data tells the Government something about a narrow window into one’s life. But gathering data from six different days, over five weeks, is much more intrusive. Individuals have an expectation of privacy in CSLI of anything more than six consecutive hours and seeking that data requires a *probable cause* warrant.

The safe harbor rule is an outgrowth of the mosaic theory. “Under the mosaic theory, while each individual

piece of information collected may not amount to a search, the cumulative, aggregate nature of the data collected may.” *Commonwealth v Henley, et al.* (SJC-12951 August 5, 2021), *citing* Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 320 26 (2012). “Whether the aggregation of data collected by police implicates the mosaic theory depends on how much data police retrieved, and the time period involved.” *Ibid.* For example, in *Henley*, this Court recently decided that seeking only two days of MBTA travel history and surveillance video was not a “search” in the constitutional sense. *Ibid*; *but see e.g. Commonwealth v. Mora*, 485 Mass. 360, 364 (2020) (long duration of pole camera surveillance required warrant).

It cannot be overstated that the “safe harbor” rule, and the mosaic theory, govern the relationship between the government and one person—specifically a suspect. None of these cases have dealt with the kind of data mining at issue here, where the government has no suspect but, rather, wants to fish through the technological fingerprints of tens



of thousands of innocent persons suspected of no wrongdoing whatsoever.

Perry concedes there is some limited amount of CSLI data for which the government need not obtain a probable cause warrant, be it the six-hour safe harbor rule or something less after *Carpenter*. But that concession only applies to the government's efforts with respect to *a suspect*. Perry does not concede there can ever be a safe harbor rule, or a warrant, that would authorize what the Government did here.

Allowing the government to fish for the staggering amount of data in this case eviscerates societal expectations of privacy. Society is willing to accept that a suspect has diminished expectations of privacy—as compared to an innocent person. Society is not willing to accept that technological advancements mean it collectively surrenders its privacy so that the government can investigate a case with no leads.

On an individual basis, this intrusion may not seem too egregious. But it is. It is because the government is spying on innocent persons; it is because the government is amassing databases it can use later; it is because allowing this now starts the slippery slope that leads to greater privacy intrusions later. The framers never envisioned that the constitution would be interpreted to allow mass surveillance of the general population.

Applying the safe harbor rule (or the mosaic theory) to validate the government's conduct because it did not intrude too much on any individual, even though it intruded collectively on tens of thousands of innocent individuals, is the exception that swallows fourth amendment (and article 14) protections against general warrants.

*E. Orders authorizing searches of an unspecified number of persons and/or phone numbers are general warrants.*

It should be plainly clear what the government cannot do. Any authorization to search telephone CSLI of anything more than an identified individual's specific phone is an

unconstitutional general warrant—be it a probable cause or § 2703(d) warrant. The privacy burdens these warrants impose are significant.

These warrants do not give the public notice, either before the police seek the data, or after; rather, the public is left to wonder if the government is watching. *Cf.*

*Commonwealth v. Amaral*, 398 Mass. 98, 100 (1986)

(“Although not an indispensable precondition to the reasonableness of a roadblock, advance publication of the date (but not the precise location) of an intended roadblock will serve both to increase its deterrent effect and to decrease its subjective impact on individuals.”). Without notice, persons caught up in the search have no recourse to contest the order, confront the Commonwealth, or seek some other redress to prevent the government from seeing or using their data.

Massachusetts law values privacy. Government agencies shall “not collect or maintain more personal data than are reasonably necessary for the performance of [their]

statutory functions.” *See Commonwealth v. Amato*, 80 Mass. App. Ct. 230, 236 (2011) *quoting* General Laws c. 66A, § 2(l). When they do, they can be sued; but only someone who has notice can sue. These warrants allow the Government to collect more personal data than is “reasonably necessary”<sup>4</sup> while shielding itself from liability.

Additionally, the information gathered is not trivial. “A person does not surrender all Fourth Amendment protection by venturing into the public sphere[,] [f]or ‘what [someone] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.’” *McCarthy*, at 501 (citations omitted). Telephone CSLI allows the Government to track innocent, non-suspecting people in constitutionally protected areas, such as “the abortion clinic, the AIDS treatment center, the strip club,

---

<sup>4</sup> The warrants returned data which included not just the cell phone in the vicinity of the cell tower, but also the phone number dialed (or that dialed it) and whether it was a phone call or a text message. That information is not necessary to determine which cell phones were in the vicinity of the crime areas.

the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, [or] the gay bar.” *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). And the Government does this without notifying individuals, “alter[ing] the relationship between citizen and government in a way that is inimical to democratic society.” *Id.* at 417. As this Court already acknowledged, “we imagine Massachusetts residents would object were the police continuously to track every person’s public movements by traditional surveillance methods, absent any suspicion at all.” *Commonwealth v. McCarthy*, 489 Mass. at 500.

Contrary to the motion judge’s conclusion that these warrants “did not involve intruding into any non-public space,” they absolutely tracked persons indoors—which is not a public place.

In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone—almost a “feature of human anatomy,”—tracks nearly exactly the

movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.

*Carpenter v. U.S.*, 138 U.S. 2206, 2218 (2018) (citations omitted).

Finally, like many investigative “innovations,” it is likely to burden populated cities, and minority communities, the most.

“[Mass surveillance] touches everyone, but its hand is heaviest in communities already disadvantaged by their poverty, race, religion, ethnicity, and immigration status.” While technology “allow[s] government watchers to remain unobtrusive,” the impact of surveillance “[is] conspicuous in the lives of those least empowered to object.” Because those communities are over-surveilled, they tend to be over-policed, resulting in inflated arrest rates and increased exposure to incidents of police violence.

...

Too often today, liberty from governmental intrusion can be taken for granted in some

neighborhoods, while others “experience the Fourth Amendment as a system of surveillance, social control, and violence, not as a constitutional boundary that protects them from unreasonable searches and seizures.”

*Leaders of a Beautiful Struggle v. Baltimore Police*

*Department*, 2 F.4th 330 (4<sup>th</sup> Cir. 2021) (citations omitted)

(finding the Aerial Investigation Research (“AIR”) program unconstitutional).

Massachusetts is not immune to the phenomenon of over-policing:

In Massachusetts, a report on the Boston Police Department’s civilian encounters between 2007 and 2010 showed that despite making up only 24% of Boston’s population, Black people were subject to 63% of reported encounters where Boston police officers interrogated, stopped, frisked, or searched a civilian. Latinx people, despite making up only 12% of Boston’s population, were subject to approximately 18% of such encounters. Another study of the Boston Police Department’s traffic stops found that Black and Hispanic drivers were more than twice as likely as White drivers to have their car searched as part of a traffic stop. The study’s modeling suggested that the disparity in searches was more consistent with racial bias than with differences in criminal conduct.

See Elizabeth Tsai Bishop, etl a., Harvard Law School, Criminal Justice Policy Program, *Racial Disparities in the Massachusetts Court System*, 18-19 (2020).

Yet, there is no reason for concern as long as this Court assures that all probable cause and § 2703(d) warrants comply with the constitutional requirements of particularity and nexus.

- i. Warrants that knowingly sweep up countless innocent persons lack particularity.

Broad warrants like these violate the particularity clause that protects against unfettered rummaging. Just as the Commonwealth cannot justify searching “all persons” present when it executes a warrant for a specific suspect or location, nor can it search “all telephone CSLI” of persons present where a crime took place.

The potential to use [CSLI] to identify a wrongdoer by identifying everyone (or nearly everyone) at the time and place of a crime may be tempting. But if the government can identify that wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials to “rummage where they please in order to see what turns up,” [*United States v. Sanchez-*



*Jara*, 889 F.3d 418, 421 (7th Cir. 2018)], even if they have reason to believe something will turn up, a [ ] court in the United States of America should not permit the intrusion. Nowhere in Fourth Amendment jurisprudence has the end been held to justify unconstitutional means.

*Matter of Search of Information Stored at Premises*

*Controlled by Google*, 481 F.Supp.3d at 757.

Searching innocent, uninvolved persons is antithetical to the constitutional protections against arbitrary government power. That is why “all person” warrants are unconstitutional (unless there is probable cause for every person present). *Commonwealth v. Smith*, 370 Mass. 335, 346 (1976). That is also why building-wide warrants are unconstitutional. “A warrant which directs the search of an entire multiple occupancy building, when probable cause exists to search only one or more separate dwelling units within the building, is void because of the likelihood that all units within the dwelling will be subjected to unjustified and indiscriminate search.” *See Commonwealth v. Erickson*, 14 Mass. App. Ct. 501, 504 (1982). If “all person” and building-wide warrants are unconstitutional, then so are

tower dump warrants. Like in those cases, the government here could not assure that everyone caught up in the tower dump was a suspect; quite the contrary, the government assured that all but one was innocent.

The privacy implications at issue here are significant. It may be that an individual—who, whether he knows it or not, is a suspect in a crime—has a diminished expectation of privacy in a limited search of his CSLI data. However, when the data sought includes potentially thousands of innocent persons, the privacy balance tips entirely against such Government action.

This interest is not diminished but, rather, heightened by the fact that most people carry cellular telephones with them at practically all times. “We cannot accept the proposition that [cellular telephone] users volunteer to convey their location information simply by choosing to activate and use their [cellular telephones] and to carry the devices on their person.”

...

“Awareness that the Government may be watching chills associational and expressive freedoms.” To know that the government can find you, anywhere, at any time is -- in a word -- “creepy.” “It is a power that places the liberty of

every [person] in the hands of every petty officer[.]”

*Commonwealth v. Almonor*, 482 Mass. 35, 54-55 (2019)

(Lenk, J. concurring) (citations omitted). In short, “people do not buy cell phones to serve as tracking devices or reasonably expect them to be used by the government in that way.” *State v. Earls*, 214 N.J. 564, 568-69 (2013).

Recall, in this case, the government later determined that one of the dates for which it sought data was not connected to its investigation. That information now lives in a police database and no one who was caught up in it has any idea or will likely ever find out.

- ii. Without information that a phone had been used during the crimes, the affidavit did not provide the requisite nexus to establish probable cause nor “reasonable belief” under § 2703(d).

There is another aspect to this case that presents a stark departure from precedent. In every case where the government had an identified suspect and phone number, it also had information that the suspect used a cell phone during the crime. *See e.g. Hobbs*, at 548-49 (“In the instant

case, the affidavit demonstrated probable cause that the defendant committed the killing, *and also established that he possessed a cell phone*. . . These facts demonstrated the requisite nexus between the CSLI and the killing.”)

(emphasis added); *Augustine*, (defendant made numerous calls to the victim, and others, before, during and after the crime occurred); *Jordan*, 91 Mass. App. Ct. 743 (video footage of suspect showed him holding what appeared to be a cell phone at the scene of the crime). Information that the suspect used a phone is indispensable in the probable cause/reasonable belief analysis.

It is indispensable because probable cause requires a “nexus” between what is being sought and where it is being searched for. *Snow* 486 Mass. at 588-89, *quoting Commonwealth v. Matias*, 440 Mass. 787, 794 (2004). In cases of CSLI, the government is seeking evidence of one’s presence by looking at where their phone was at the time of the crime. If the police cannot connect a suspect to “ownership of a particular device” and his “location at or

around the time the crime was committed,” there is not probable cause (nor reasonable belief) to obtain CSLI data.<sup>5</sup> See *Matter of Search of Information Stored at Premises Controlled by Google*, 481 F.Supp.3d at 757; *Commonwealth v. Vasquez*, 482 Mass. 850, 867 (2019). In *Vasquez*, for example, the suspect had been identified by family members as being at the scene of the crime. And yet, even then, without specific information that he possessed a phone at the scene of the crime, that was not enough to establish probable cause. *Id.*

This Court has repeatedly instructed that an unsupported opinion is not enough. “[W]here the location of the search or seizure is a computer-like device, such as a cellular telephone, the opinions of the investigating officers do ‘not, alone, furnish the requisite nexus between the criminal activity and the [device] to be searched’ or seized.” *Commonwealth v. White*, 475 Mass. 583, 589 (2016), *quoting*

---

<sup>5</sup> And, of course, to comply with particularity, it must establish who the suspect is and what is the target telephone number.

*Commonwealth v. Anthony*, 451 Mass. 59, 72, (2008). Yet that is all there was here. The government did not have any evidence the suspect possessed a phone during the robberies. The judge simply credited the affidavits in support of the warrants that “most people use cell phones and keep them on them.”

However, the “police may not rely on the general ubiquitous presence of cellular telephones in daily life, or an inference that friends or associates most often communicate by cellular telephone, as a substitute for particularized information that a specific device contains evidence of a crime.” *Commonwealth v. Morin*, 478 Mass. 415, 426 (2017). Nor is it enough to opine “that coventurers often use cell phones to communicate . . .” See *Commonwealth v. Snow*, 486 Mass. 582, 589 (2021), discussing *White*, at 588. It is not even enough “to show that the defendant communicated with a person implicated in the crime via cell phone.” *Commonwealth v. Louis*, 487 Mass. 759, 764 (2021).

The only time this Court has allowed a warrant on less than direct observations that a suspect used a phone during the crime was in *Commonwealth v Henley, et al.* (SJC-12951 August 5, 2021). *Henley* could be read as relaxing the nexus standard between a phone and a crime. Nevertheless, *Henley* is distinguishable for several important reasons.

First, the affidavit in *Henley* was much more detailed and established many more specific, compelling facts to imply a phone was used than in this case.

We emphasize that this case presents a highly unusual combination of factors: there was no apparent instigating event for the murder; two rival gang members, one of whom was the victim, were part of the same work crew at the time of the murder; and, finally, another rival gang member of the victim, who did not live near the work site or have any plausible reason to be there, arrived at the work site at around the time of murder.

*Henley*, at \*41. None of those facts were present here. The affidavit here was based on the kind of conjecture this Court has previously rejected.

Secondly, and more importantly, in *Henley*, the police sought to search the phone of a suspect it had in custody. *Henley* is an extension of this Court's myriad cases where the government is investigating an "identified individual." To emphasize again, in this case, there was no "identified individual." The government wanted to search for CSLI data of tens of thousands of innocent persons because the suspects probably used a phone and, well, so does everyone else. That is a bridge too far.

If the Commonwealth was wrong about *Henley*, it would have intruded on his privacy. But it would have intruded *only* on this one person's privacy. Whenever the government is seeking the kind of data it sought here, it will knowingly be intruding on the privacy rights of tens of thousands of innocent persons. The nexus requirement in a case like this must be clearer than the nexus requirement in a case like *Henley*.

Requiring more than an assumption that a phone was used during the commission of the crime prevents CSLI



warrants from becoming general warrants. It assures that the government is not just guessing that it may find something, just like the British soldiers went to every home hoping to find untaxed goods. Rather, it upholds the constitutionally required nexus component to any warrant.

### CONCLUSION

The warrants executed here were clearly unconstitutional general warrants. This Court should not sanction such broad, sweeping searches. Accordingly, the evidence from the warrants, and the fruits of these searches, must be suppressed.

Respectfully submitted,

/s/ Eric Tennen  
Eric Tennen, B.B.O. No. 650542  
Swomley & Tennen, LLP  
50 Congress Street, Ste 600  
Boston, MA 02109  
Tel. 617-227-9443  
etennen@swomleyandtennen.com

# **ADDENDUM**

## **U.S. Constitution, Amendment IV**

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

## **Massachusetts Declaration of Rights, Article 14**

Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.

.

## **18 U.S.C. § 2703(d)**

### **(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 and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under

section 846 of that title, in accordance with regulations prescribed by the President) 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.

...

**(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.

## **M.G.L. c. 66A, § 2**

### **Holders maintaining personal data system; duties**

Every holder maintaining personal data shall:—

- (a) identify one individual immediately responsible for the personal data system who shall insure that the requirements of this chapter for preventing access to or dissemination of personal data are followed;
- (b) inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the personal data system, or the use of any personal data contained therein, of each safeguard required by this chapter, of each rule and regulation promulgated pursuant to section three which pertains to the operation of the personal data system, and of the civil remedies described in section three B of chapter two hundred and fourteen available to individuals whose rights under chapter sixty-six A are allegedly violated;
- (c) not allow any other agency or individual not employed by the holder to have access to personal data unless such access is authorized by statute or regulations which are consistent with the purposes of this chapter or is approved by the data subject whose personal data are sought if the data subject is entitled to access under clause (i). Medical or psychiatric data may be made available to a physician treating a data subject upon the request of said physician, if a medical or psychiatric emergency arises which precludes the data subject's giving approval for the release of such data, but the data subject shall be given notice of such access upon termination of the emergency. A holder shall provide lists of names and addresses of applicants for professional licenses and lists of professional licensees to associations or educational organizations recognized by the appropriate professional licensing or examination board. A holder shall comply with a data subject's request to

disseminate his data to a third person if practicable and upon payment, if necessary, of a reasonable fee; provided, however, that nothing in this section shall be construed to prohibit disclosure to or access by the bureau of special investigations to the records or files of the department of transitional assistance for the purposes of fraud detection and control;

(d) take reasonable precautions to protect personal data from dangers of fire, identity theft, theft, flood, natural disaster, or other physical threat;

(e) comply with the notice requirements set forth in section sixty-three of chapter thirty;

(f) in the case of data held in automated personal data systems, and to the extent feasible with data held in manual personal data systems, maintain a complete and accurate record of every access to and every use of any personal data by persons or organizations outside of or other than the holder of the data, including the identity of all such persons and organizations which have gained access to the personal data and their intended use of such data and the holder need not record any such access of its employees acting within their official duties;

(g) to the extent that such material is maintained pursuant to this section, make available to a data subject upon his request in a form comprehensible to him, a list of the uses made of his personal data, including the identity of all persons and organizations which have gained access to the data;

(h) maintain personal data with such accuracy, completeness, timeliness, pertinence and relevance as is necessary to assure fair determination of a data subject's qualifications, character, rights, opportunities, or benefits when such determinations are based upon such data;

(i) inform in writing an individual, upon his request, whether he is a data subject, and if so, make such data fully

available to him or his authorized representative, upon his request, in a form comprehensible to him, unless doing so is prohibited by this clause or any other statute. A holder may withhold from a data subject for the period hereinafter set forth, information which is currently the subject of an investigation and the disclosure of which would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest, but this sentence is not intended in any way to derogate from any right or power of access the data subject might have under administrative or judicial discovery procedures. Such information may be withheld for the time it takes for the holder to complete its investigation and commence an administrative or judicial proceeding on its basis, or one year from the commencement of the investigation or whichever occurs first. In making any disclosure of information to a data subject pursuant to this chapter the holder may remove personal identifiers relating to a third person, except where such third person is an officer or employee of government acting as such and the data subject is not. No holder shall rely on any exception contained in clause Twenty-sixth of section seven of chapter four to withhold from any data subject personal data otherwise accessible to him under this chapter;

(j) establish procedures that (1) allow each data subject or his duly authorized representative to contest the accuracy, completeness, pertinence, timeliness, relevance or dissemination of his personal data or the denial of access to such data maintained in the personal data system and (2) permit personal data to be corrected or amended when the data subject or his duly authorized representative so requests and there is no disagreement concerning the change to be made or, when there is disagreement with the data subject as to whether a change should be made, assure that the data subject's claim is noted and included as part of the data subject's personal data and included in any subsequent disclosure or dissemination of the disputed data;

(k) maintain procedures to ensure that no personal data are made available in response to a demand for data made by means of compulsory legal process, unless the data subject has been notified of such demand in reasonable time that he may seek to have the process quashed;

(l) not collect or maintain more personal data than are reasonably necessary for the performance of the holder's statutory functions.

### **Mass. R. Crim. P. 13(a)(2)**

#### **Grounds and affidavit**

A pretrial motion shall state the grounds on which it is based and shall include in separately numbered paragraphs all reasons, defenses, or objections then available, which shall be set forth with particularity. If there are multiple charges, a motion filed pursuant to this rule shall specify the particular charge to which it applies. Grounds not stated which reasonably could have been known at the time a motion is filed shall be deemed to have been waived, but a judge for cause shown may grant relief from such waiver. In addition, an affidavit detailing all facts relied upon in support of the motion and signed by a person with personal knowledge of the factual basis of the motion shall be attached.



COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT  
CRIMINAL ACTION  
NO. 1984CR00396

COMMONWEALTH

vs.

JERRON PERRY

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

The defendant, Jerron Perry (“Perry”), moved to suppress essentially all of the evidence against him, arguing that the evidence is the fruit of two unconstitutional searches of cell phone company tower records and related phone information, searches that are often called cell tower dumps.<sup>1</sup> Both searches were conducted pursuant to search warrants. Perry argues that the warrant applications lacked probable cause and that the warrants, which covered extensive cell phone information unconnected to any suspect, were overbroad and unparticularized “general warrants.” The Court heard oral argument on February 18, 2021. For the reasons stated below, the defendant’s motion is **DENIED**.

FINDINGS OF FACT

Between September 22, 2018 and October 31, 2018, five armed robberies and one attempted armed robbery resulting in a fatal shooting occurred in the Dorchester and Mattapan sections of Boston and in Canton. All six incidents had similarities, including the perpetrator’s height, size and clothing, and certain circumstances of the offenses. Federal and state

---

<sup>1</sup> Perry also challenged a search warrant for Google tower records. However, because no evidence obtained from that warrant was used in any subsequent search warrant, the Court does not address the related issue of Google tower warrants.

investigators conducted an extensive investigation including obtaining the two search warrants that are challenged in this motion.

**1. The October 26, 2018 search warrant.**

On October 26, 2018, after several of the six incidents had occurred, a federal agent sought and obtained a search warrant from a federal magistrate judge pursuant to the federal Stored Communications Act, 18 U.S.C. § 2703. The warrant sought historical cell site location information (“CSLI”) and other cell phone information connected to four robberies<sup>2</sup> from AT&T Wireless, Sprint/Nextel, T-Mobile, and Verizon Wireless, four companies that have cell phone towers in the Greater Boston area. The historical CSLI consisted of the unique identifiers of those cell phones that had communicated with each company’s tower that was closest to the scene of each crime, during 15-minute time periods spanning from shortly before to shortly after each incident. For each communication that had occurred during that time period, including those that began before or ended after that period, the warrant also sought source and destination telephone numbers; date, time, and duration of the communication; sector (face of the tower); and type of communication, e.g., text, phone call.

**2. The January 30, 2019 search warrant.**

On January 30, 2019, after all six of the incidents had occurred, a Boston police detective sought and obtained a search warrant from a Superior Court judge pursuant to G. L. c. 276, §§ 1-7. This second warrant sought the same types of cell phone information from the same four companies, including historical CSLI from all cell phones that had communicated with each company’s tower that was closest to the scene of each crime. The second warrant covered 40-minute time periods spanning shortly before to shortly after each incident.

---

<sup>2</sup> In addition to the three incidents relevant to this motion, the warrant application discussed a fourth robbery that had occurred in Cambridge and that the Commonwealth later decided could not definitively be linked to Perry.

**3. Asserted basis for probable cause in the two warrants.**

The affidavits supporting the warrant applications do not identify a suspect by name. Nor do they include any evidence that the perpetrator or perpetrators used a cell phone during the relevant time periods. Probable cause is based on the fact that (1) almost everyone has a cell phone and carries it with them; (2) most cell phones record one's whereabouts, even when not being actively used; (3) based on similarities between the offenses as set forth in the affidavits, it is likely that the same person committed all six crimes, possibly with one or more co-venturers; and (4) it is therefore likely that the same cell phone was in the vicinity of several or all of the six incidents.

**4. Use of cell phone information and subsequent searches.**

The cell phone information obtained from the warrants included two phone numbers that police detectives and federal agents linked to the crimes. The first, telephone number 857-417-3393 (identified as "Target Device 1"), was a phone number that Perry had provided to police in January 2018 after a traffic accident. By the time the second warrant was obtained, Canton police had identified Perry as a possible suspect in the two robberies that had occurred in Canton, on September 27, 2018 and October 31, 2018. Target Device 1 had been in the vicinity of the October 6, 2018 attempted robbery and fatal shooting in Dorchester, and at the October 31, 2018 robbery in Canton, at the time of those incidents.

The cell phone records obtained from the two warrants revealed a phone call between Target Device 1 and telephone number 857-271-9234 (identified as "Target Device 2") at the time of the attempted robbery and fatal shooting. The records further revealed that Target Device 2 had been in the vicinity of the October 6, 2018 attempted robbery and fatal shooting in

Dorchester, the October 31, 2018 robbery in Canton, and the September 22, 2018 robbery in Mattapan, all at the time of those incidents.

Based on this information and additional investigation, police identified Perry and co-venturer Gregory Simmons as suspects in the robberies. Subsequent investigation by police and agents, including subsequent warrants, led to Perry's indictment on murder and other charges.

## DISCUSSION

### **1. Perry Has Sufficiently Complied with Mass. R. Crim. P. 13**

The Commonwealth argues that the absence of an affidavit from Perry is fatal under Rule 13(a)(2). The Court rejects this argument.

Rule 13(a)(2) requires that “an affidavit detailing all facts relied upon in support of the motion and signed by a person with personal knowledge of the factual basis of the motion shall be attached” to a pretrial motion. An affidavit from counsel can satisfy the rule. See *Commonwealth v. Santosuosso*, 23 Mass. App. Ct. 310, 313 (1986) (affidavit by counsel sufficient).

“[T]he purpose of the affidavit requirement ... is: (1) to give the judge considering the motion a statement of anticipated evidence, in reliable form, to meet the defendant's initial burden of establishing the facts necessary to support his motion..., and (2) to provide the Commonwealth with fair notice of the specific facts relied on in support of the motion set forth in a form, i.e., under oath, which is not readily subject to change by the affiant.” *Id.* (internal citations omitted). Because this is a “four corners” challenge to search warrants, counsel's affidavit satisfies both purposes. See *Commonwealth v. Mubdi*, 456 Mass. 385, 389–390 (2010); *Commonwealth v. Fudge*, 20 Mass. App. Ct. 382, 386 (1985).

## **2. Perry Has Standing**

The Commonwealth argues that Perry does not have standing or a reasonable expectation of privacy to challenge the search. But the Supreme Judicial Court (“SJC”) has recognized that one has a reasonable expectation of privacy in one’s cell phone location, see *Commonwealth v. Augustine*, 467 Mass. 230, 255 (2014), and has further stated that “[e]vidence may be suppressed as fruit of the poisonous tree even if it is found in a place where the defendant has no reasonable expectation of privacy.” *Commonwealth v. Fredericq*, 482 Mass. 70, 78 (2019). Moreover, the SJC has specifically held that suppression of subsequently-obtained evidence must be suppressed when that evidence was “based directly on the tainted CSLI.” *Commonwealth v. Estabrook*, 472 Mass. 852, 864 (2015). Therefore, the Court must decide whether police lawfully obtained the CSLI at issue in this case based on the two challenged warrants and the supporting affidavits.

## **3. The Affidavits Established Probable Cause to Issue the Cell Tower Warrants**

It appears that neither the SJC nor the Appeals Court has directly addressed the issue of CSLI obtained from cell tower dump or other “geofence” warrants. See, e.g., Cypher, Geofence Warrants, 30 Mass. Prac., Criminal Practice & Procedure § 5:166 (4th ed.) (March 2021 Update).<sup>3</sup> Moreover, the parties have cited no Superior Court case directly on point, and this Court is not aware of any such case.

The Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights require that a warrant be based on probable cause. *Commonwealth v. Morin*, 478 Mass. 415, 425 (2017).<sup>4</sup> Probable cause requires law enforcement to “have ‘a

---

<sup>3</sup> Justice Cypher defines geofence warrants as warrants that “collect the location data of every electronic device in a specified area during a specified time period.” *Id.*

<sup>4</sup> Although federal courts may use a less-demanding standard pursuant to 18 U.S.C. § 2703, see *Commonwealth v. Augustine*, 467 Mass. 230, 236 (2014), probable cause is required in Massachusetts to obtain CSLI. See *Commonwealth v. Hobbs*, 482 Mass. 538, 543 (2019).

substantial basis for concluding that 'the item searched or seized contains 'evidence connected to the crime' under investigation.'" *Commonwealth v. White*, 475 Mass. 583, 588 (2016), quoting *Commonwealth v. Escalera*, 462 Mass. 636, 642 (2012). It does not require a *likelihood* that evidence of a crime will be present:

The probable cause standard does not require a showing that evidence more likely than not will be found; in other words, it is not equivalent to a preponderance of the evidence standard. Rather, "probable cause" means merely that quantum of evidence from which the magistrate can conclude, applying common experience and reasonable inferences, that items relevant to apprehension or conviction are reasonably likely to be found at the location.

*Commonwealth v. Murphy*, 95 Mass. App. Ct. 504, 509, *review denied*, 483 Mass. 1102 (2019), citing *Texas v. Brown*, 460 U.S. 730, 742 (1983) (probable cause "does not demand any showing" that belief that contraband is at location is "more likely true than false"); see also *Hobbs*, 482 Mass. at 544 (inferences drawn from affidavit need not be more likely true than not). This standard applies when, as in this case, the government seeks a warrant for historical CSLI.<sup>5</sup> *Augustine*, 467 Mass. at 255-256.

Implicit in the showing of probable cause in this context is the unlikelihood that someone *not* involved in the robberies and attempted robbery would happen to have been close to the scene of two or more crimes that occurred in Boston and Canton or different parts of Boston.<sup>6</sup> The Court credits statements in the supporting affidavits from experienced law enforcement officers that most people use cell phones and keep them on. Therefore, there was a "substantial basis", see *White*, 475 Mass. at 588, to conclude that the historical CSLI obtained through these

---

<sup>5</sup> In limited circumstances not applicable here, a warrant is unnecessary when no search in the constitutional sense occurred. See *Hobbs*, 482 Mass. at 544 n. 9.

<sup>6</sup> Not surprisingly, the cell phone numbers of numerous non-suspects were in the vicinity of more than one of the three robberies that occurred in the same Mattapan neighborhood.

searches would identify one or more common denominator cell phone numbers, i.e., numbers for cell phones that were in the vicinity of two or more crimes that occurred in different areas.

In sum, because as a means to investigate the robberies and other crimes there was a “substantial basis,” *id.*, to conclude that the “CSLI sought will produce evidence of such offense[s] or will aid in the apprehension of a person who the applicant has probable cause to believe has committed such offense[s],” *Augustine*, 467 Mass. at 236 n. 15 (internal alteration and quotation omitted), the warrants were supported by probable cause.

#### **4. The Warrants Were Not Overbroad, Unparticularized “General Warrants”**

Both art. 14 and the Fourth Amendment “were enacted, in large part, in response to the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.” *Commonwealth v. Mora*, 485 Mass. 360, 370 (2020) (internal quotations omitted). A “general warrant” refers to a warrant providing law enforcement with broad authority to search and seize unspecified places or persons. See *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018). A warrant must “particularly describe the items to be seized.” *Massachusetts v. Sheppard*, 468 U.S. 981, 987 (1984).

In *Commonwealth v. McCarthy*, 484 Mass. 493 (2020), the SJC addressed the concern over general warrants in the context of digital information:

The surveillance implications of new technologies must be scrutinized carefully, lest scientific advances give police surveillance powers akin to these general warrants. Just as police are not permitted to rummage unrestrained through one's home, so too constitutional safeguards prevent warrantless rummaging through the complex digital trails and location records created merely by participating in modern society.

*Id.* at 499. In *Commonwealth v. Wilkerson*, 486 Mass. 159 (2020), the SJC held that “where a warrant so lacks particularity or is so overbroad that it begins to resemble a general warrant, total

suppression is required.” *Id.* at 169. Accordingly, courts must be wary when reviewing warrants for large amounts of digital data. See, e.g., *id.* (holding, as applied to CSLI, the “forty-eight hours requested, and the thirty-four hours obtained here, are not so overbroad on the facts of this case so as to be akin to a general warrant”); *Commonwealth v. Gosselin*, 486 Mass. 256, 263 (2020) (expressing concern against digital “rummaging”).

In assessing searches for digital information, courts must consider the surreptitious nature of the intrusion and the extent of the intrusion, measured in terms of duration and the amount and nature of the information obtained. See *McCarthy*, 484 Mass. at 499-500; *Wilkerson*, 486 Mass. at 169; *Mora*, 485 Mass. at 374-375. Moreover, the Fourth Amendment protects against the aggregation of limited surveillance activities that, in total, reveal a complex, intrusive picture of a suspect’s life. See *McCarthy*, 484 Mass. at 502–504 (discussing “mosaic theory” of Fourth Amendment such that, at a certain point, limited surveillance can be aggregated to reveal a complex picture of an individual life); *Carpenter*, 138 S. Ct. at 2217–2218 (similar).

The targeted and temporally-limited searches in this case (which effectively are one search for a very limited number of common denominators) are a far cry from those that offer an “intimate window into a person’s life” that the Fourth Amendment and art. 14 protect in the digital age. See *Carpenter*, 138 S. Ct. at 2217; accord *McCarthy*, 484 Mass. at 503–504. Indeed, measured by the above-noted criteria, the challenged searches fall at the permissible end of a spectrum that ranges from targeted, relatively non-intrusive searches in public places to broad, intrusive, unconstitutional rummaging through a suspect’s home or other private space. The Court has specifically considered five aspects of the warrants at issue in this motion.

*First*, although the intrusion was surreptitious to anyone unaware of how CSLI is collected, it did not involve intruding into any non-public space. Moreover, most cell phone



users are aware at least to some extent that their locations are conveyed to cell phone providers in order to receive cell phone service. See *Commonwealth v. Almonor*, 482 Mass. 35, 46 (2019).

*Second*, the nature of the information collected here was non-invasive, consisting of historical CLSI and phone numbers, not names or other personal identifying information, and the type of communication (e.g. text, cell phone), not the content of any communication. While users' locations were identified, they were anonymous with no or limited tracking of movement.

*Third*, the searches were extremely limited temporally, involving only 15 minutes or 40 minutes of time. This was the opposite of a "mosaic," in which limited surveillance is aggregated to reveal a complex picture of an individual life. See *McCarthy*, 484 Mass. at 508-509 (limited number of cameras in public not enough to trigger mosaic theory concern); contrast *Commonwealth v. Snow*, 486 Mass. 582, 593 (2021) (holding that a lack of a temporal limit on a warrant rendered it "not sufficiently particular" due to the vast amount of information a cell phone can hold).

*Fourth*, law enforcement officers provided detailed affidavits explaining a nexus to criminality and why the sought information would be useful in identifying one or more suspects. See *Hobbs*, 482 Mass. at 544 (holding that a search warrant for CSLI must be based on probable cause that "a particular offense has or will be committed" and that the CSLI will produce evidence of that offense); *Snow*, 486 Mass. at 586 (similar in context of phone search).

*Fifth*, although the warrants were broad in the sense of capturing extensive information that federal agents and detectives knew would not be needed for further investigation, they were not *overbroad* because there was no less intrusive way to identify the suspects in the crimes under investigation, i.e., a string of robberies and an attempted robbery that led to a fatal shooting. See *Wilkerson*, 486 Mass. at 169. Without the name or phone number of a suspect,

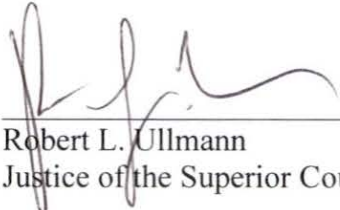
law enforcement officers did not know which of the four cell phone companies provided cell phone service to any suspect who had a cell phone. Moreover, as noted above, all of the locations and timeframes were closely targeted to the scene and time of the crimes.

In sum, the warrants obtained here have the scope and particularity of constitutional warrants, not unconstitutional “general warrants.” The acquisition of historical CSLI and related cell phone information in the manner and for the purpose described herein does not violate the Fourth Amendment or art. 14, and consequently no evidence derived from the execution of the warrants must be suppressed.

**CONCLUSION AND ORDER**

For the above reasons, Defendant’s Motion to Suppress Evidence Obtained from Cellular Towers Pursuant to Search Warrant (Paper #20) is **DENIED**.

Dated: April 21, 2021

  
\_\_\_\_\_  
Robert L. Ullmann  
Justice of the Superior Court

## CERTIFICATE OF COMPLIANCE

I hereby certify that, pursuant to Mass. R. App. P. 16(k), the foregoing brief complies with the rules of court pertaining to the filing of briefs. This brief complies with the type-volume limitation of Mass. R. App. P. 20(a)(2)(A) because it was prepared in Microsoft Word and contains 7561 words, 0 excluded, in the proportionally spaced Century Schoolbook 14-point font.

/s/ Eric Tennen  
Eric Tennen

## CERTIFICATE OF SERVICE

I hereby certify that service of the foregoing brief and accompanying Record Appendix was made on the attorney of record for the Commonwealth, Cailin Campbell, by the Electronic Filing System this 18th day of August, 2021 by sending to:

Cailin.campbell@state.ma.us  
jennifer.hickman@state.ma.us

/s/ Eric Tennen  
Eric Tennen  
B.B.O. No. 650542  
Swomley & Tennen, LLP  
50 Congress Street, Ste 600  
Boston, MA 02109  
Tel. 617-227-9443  
etennen@swomleyandtennen.com