SJC-13144

COMMONWEALTH vs. JERRON PERRY.

Suffolk. December 8, 2021. - April 1, 2022.

Present: Budd, C.J., Gaziano, Lowy, Cypher, Kafker, Wendlandt, & Georges, JJ.

Cellular Telephone. Constitutional Law, Search and seizure, Privacy, Probable cause, Retroactivity of judicial holding. Search and Seizure, Expectation of privacy, Warrant, Affidavit, Probable cause. Privacy. Probable Cause. Practice, Criminal, Motion to suppress, Warrant, Affidavit, Retroactivity of judicial holding. Retroactivity of Judicial Holding.

Indictments found and returned in the Superior Court Department on July 12, 2019.

A pretrial motion to suppress evidence was heard by Robert L. Ullmann, J.

An application for leave to prosecute an interlocutory appeal was allowed by Georges, J., in the Supreme Judicial Court for the county of Suffolk, and the case was reported by him.

Eric Tennen for the defendant.

Cailin M. Campbell, Assistant District Attorney (Jennifer J. Hickman, Assistant District Attorney, also present) for the Commonwealth.

Mason A. Kortz, for Surveillance Technology Oversight Project, amicus curiae, submitted a brief.

Brett Max Kaufman, Ashley Gorski, & Patrick Toomey, of New York, Jennifer Granick, Jennifer Lynch, & Andrew Crocker, of California, Matthew Spurlock, Committee for Public Counsel Services, Matthew R. Segal, Jessie J. Rossman, Jessica J. Lewis, Nathan Freed Wessler, & Joshua M. Daniels, for American Civil Liberties Union & others, amici curiae, submitted a brief.

GAZIANO, J. As law enforcement capabilities continue to develop in the wake of advancing technology, so too must our constitutional jurisprudence. To this end, we must grapple with the constitutional implications of "tower dumps," a relatively novel law enforcement tool that provides investigators with the cell site location information (CSLI) for all devices that connected to specific cell towers during a particular time frame.

Here, the Commonwealth obtained search warrants for seven tower dumps,[1] corresponding to the locations of six robberies and an attempted robbery that resulted in a homicide, all of which investigators believed to have been committed by the same individual. After analyzing the information contained in the tower dumps, investigators determined that the defendant had been near the scenes of two of the crimes. The defendant subsequently was charged with the robberies and the homicide, and he moved to suppress all evidence obtained from the tower

[1] As is customary, each single tower dump included information from multiple cell towers operated by different cellular service providers. See discussion, infra.

dumps as the fruits of an unconstitutional search. A Superior Court judge denied the motion, and the defendant filed an application in the county court seeking leave to pursue an interlocutory appeal; the single justice reserved and reported the case to the full court.

The defendant argues that the Commonwealth's use of the tower dumps intruded upon his reasonable expectation of privacy, and therefore effectuated a search under the Federal and State Constitutions. He also contends that search warrants for tower dumps are per se unconstitutional because they necessarily lack particularity. In addition, the defendant asserts that, here, the warrants were not supported by probable cause.

We agree that the government's use of the seven tower dumps was an intrusion upon the defendant's reasonable expectation of privacy, and therefore constituted a search under art. 14 of the Massachusetts Declaration of Rights. We do not agree, however, that warrants for tower dumps are per se unconstitutional. Accordingly, investigators may use tower dumps so long as they comply with the warrant requirements of art. 14.

Here, the second of the two search warrants was sufficiently particular and supported by probable cause, and therefore the use of the information obtained from it does not offend the Massachusetts Declaration of Rights. The first warrant, however, was not supported by probable cause, and

accordingly, any evidence obtained as a result of it must be suppressed.[2]

1. Background. a. CSLI and tower dumps. An overview of the technology at issue is necessary to a discussion of the issues in this case. Cellular telephones "make calls, send text messages and emails, and access the internet by connecting to a set of radio antennas called 'cell sites'" (quotation and citation omitted). United States v. Thorne, 548 F. Supp. 3d 70, 113 (D.D.C. 2021). See Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018). To receive cellular service, "a cellular telephone will connect to the cell site which provides the strongest signal, typically, albeit not always, the nearest one." Commonwealth v. Jones, 477 Mass. 307, 313 n.11 (2017). "The typical cell site covers a more-or-less circular geographic area," with "three (or sometimes six) separate antennas pointing in different directions" which divide the site's radius into smaller, wedge-shaped sectors. Carpenter, supra at 2225 (Kennedy, J., dissenting).

[2] We acknowledge the amicus briefs submitted by the Surveillance Technology Oversight Project and by the American Civil Liberties Union, the American Civil Liberties Union of Massachusetts, Inc., the Committee for Public Counsel Services, the Electronic Frontier Foundation, and the Massachusetts Association of Criminal Defense Lawyers in support of the defendant.

Once a cellular telephone connects with a cell site (either to send or receive communications), the site will "generate[] a time-stamped record known as [CSLI]."[3] Id. at 2211. Among other information, this record contains the precise location of the cell site, as well the specific sectors that provided service to the cellular telephone. See Commonwealth v. Augustine, 467 Mass. 230, 237-238 (2014), S.C., 470 Mass. 837 and 472 Mass. 448 (2015) (Augustine I). When a cellular telephone establishes a connection with a particular sector of a cell site, it can be inferred that the user was located within that sector's range of service, or "coverage area," at the time of the connection. Commonwealth v. Wilkerson, 486 Mass. 159, 174 (2020). Service providers retain CSLI for their own business purposes, such as finding weak areas of their network, but it also has proved useful to law enforcement in order to approximate an individual's location at a given time. Carpenter, 138 S. Ct. at 2212.

[3] There are two forms of CSLI. See Commonwealth v. Augustine, 467 Mass. 230, 238 & n.18 (2014), S.C., 470 Mass. 837 and 472 Mass. 448 (2015) (Augustine I). Telephone call CSLI is generated only when a cellular telephone uses cell service, such as by placing or receiving a call or a text message. Id. at 238. Registration CSLI, by contrast, is created without any action by the user, as cellular telephones "regularly identify themselves to the nearest cell site with the strongest signal, through a process known as 'registration.'" Id. at 238 n.18. Only telephone call CSLI is at issue here.

The precision with which police are able to approximate an individual's location varies significantly. Some CSLI only enables investigators to place an individual within "an area miles in diameter," whereas other CSLI allows investigators to "calculate users' locations with precision that approaches that of GPS.[4]" ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong., at 23, 25 (2010) (testimony of Professor Matt Blaze) (Blaze Testimony I). The degree of precision largely depends on the size of the sector's coverage area and the technology in use. See id. at 25. The size of the coverage area, in turn, depends on the number of nearby cell sites; "[t]he greater the concentration of cell sites, the smaller the coverage area." Carpenter, 138 S. Ct. at 2211. "As cellular telephone use has grown, cellular service providers have responded by adding new cell sites to accommodate additional customers," resulting in increasingly precise CSLI. See Augustine I, 467 Mass. at 239.

CSLI also is more precise if the cell site uses newer, more advanced technology. In areas such as Boston that use what is referred to as "small cell" technology, CSLI can identify an

[4] Global positioning system.

individual's location precisely, down to the specific floor of a particular building. See State v. Earls, 214 N.J. 564, 578 (2013), quoting Blaze Testimony I, supra at 25. See also National League of Cities, Small Cell Wireless Technology in Cities, at 8-9 (2018) (discussing Boston's use of small cell technology).[5] This technology is becoming increasingly ubiquitous; "[b]y some estimates, the number of these small-scale cellular base stations equaled or outstripped the number of conventional cells in the [United States] in 2010, and their deployment continues to grow at a very fast rate." ECPA, Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 113th Cong., at 55 (2013) (testimony of Professor Matt Blaze).

In conducting a criminal investigation, law enforcement officers may obtain targeted CSLI, which provides a log of every cell site to which an individual cellular telephone has connected within a given time frame, thus enabling investigators retroactively to reconstruct an individual's movements over time. See Augustine I, 467 Mass. at 239. A tower dump, by contrast, provides officers with CSLI from every device that connected to a particular cell site within a specified period;

[5] Available at https://www.nlc.org/wp-content/uploads/2018/08/CS_SmallCell_MAG_FINAL.pdf [https://perma.cc/8CKW-KJZ8].

allowing law enforcement to infer that the owners of those devices most likely were present in that site's coverage area during that time. See Carpenter, 138 S. Ct. at 2220 (tower dump is "a download of information on all the devices that connected to a particular cell site during a particular interval"). Tower dumps have proved particularly useful in investigating serial crimes, because they enable investigators to isolate individual devices that were near the scene of multiple offenses. See Owsley, The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance, 16 U. Pa. J. Const. L. 1, 6 (2013).

b. Factual background. On September 22, September 27, September 28, October 4, October 25, and October 31, 2018, clerks at six stores in Boston, Canton, and Cambridge were robbed at gunpoint by an unidentified perpetrator. On October 6, 2018, an unidentified individual shot and killed a store clerk in Boston during an attempted robbery. Almost all of the stores were convenience stores or gasoline stations, and one sold cellular telephones. Because each of the robberies was perpetrated in a comparable manner by a man fitting a similar description, police suspected that the same person had been responsible for all seven incidents. Based on surveillance footage and witness statements, investigators also believed that

the perpetrator was at least occasionally assisted by a coventurer who acted as a getaway driver.

Boston police detectives worked together with agents from the Federal Bureau of Investigation (FBI) to identify a suspect. They sought to do so by cross-referencing a series of tower dumps in order to determine if any device had been near the scenes of two or more of the incidents. To this end, on October 26, 2018, an agent with the FBI obtained a search warrant from a Federal magistrate judge, see 18 U.S.C. § 2703, for tower dumps corresponding to the robberies in Boston, Canton, and Cambridge on September 22, September 27, September 28, and October 4, 2018 (first warrant). The first warrant required four service providers with one or more cell sites near the scenes of the robberies to produce the tower dumps. For each date, the tower dump was to include the CSLI for all cellular telephones that had connected to any cell site providing cellular service to the address where the robbery occurred, within a fifteen-minute period surrounding the time of the incident.

On January 30, 2019, a Boston police detective sought and obtained a search warrant from a judge in the Boston Municipal Court, see G. L. c. 276, §§ 1-7, for tower dumps corresponding to the robberies in Boston and Canton on October 25 and October 31, 2018, as well as the attempted robbery and homicide

in Boston on October 6, 2018 (second warrant). The application for this second warrant did not reference or otherwise rely upon any evidence obtained from execution of the first warrant. The second warrant required the same four service providers to produce the tower dumps. For each date, the tower dump was to include CSLI for all cellular telephones that had connected to any cell site serving the address where the crime occurred, within a forty-minute period around the time of each incident.

Both warrants sought the same categories of information. For each cellular telephone that connected to the relevant cell site, the providers were required to furnish (1) the location and sector of the cell site providing service; (2) the telephone number and unique identifier,[6] either of which could be used to identify the owner of the telephone; (3) the type of communication initiated or received when the connection occurred; (4) the telephone number of the device initiating the communication (known as the "source number"); (5) the telephone number of the device receiving the communication (the

[6] A "unique identifier" is a distinctive series of numbers that cellular service providers use to identify a device or its user. See Citizen Lab of the Munk School of Global Affairs at the University of Toronto, The Many Identifiers in Our Pockets: A Primer on Mobile Privacy and Security (May 13, 2015), https://citizenlab.ca/wp-content/uploads/2015/05/The-Many-Identifiers-in-Our-Pockets-A-primer-on-mobile-privacy-and-security-_reportPDF.pdf [https://perma.cc/55P6-G43X].

"destination number"); and (6) the date, time, and duration of each communication.

Collectively, execution of the search warrants produced information on over 50,000 unique telephone numbers. Investigators then cross-referenced the data from each tower dump in an effort to identify any telephone numbers that appeared in two or more of the tower dumps, and discovered that a particular telephone number appeared in the tower dump corresponding to the homicide on October 6, 2018, as well as the tower dump corresponding to the robbery on October 31, 2018. Investigators determined, by searching a police database, that this number belonged to the defendant.[7] They also learned that, at around the time of the shooting on October 6, 2018, the defendant's telephone had been in communication with another device, which they suspected to have belonged to the getaway driver. Investigators were able to determine the identity of the suspected coventurer, as well as the fact that his cellular telephone number appeared in the tower dumps corresponding to the robberies on September 22, October 6, and October 31, 2018.

[7] Following an unrelated traffic accident, the defendant previously had provided his telephone number to police.

Based on this, investigators identified the defendant as a suspect in six of the incidents, including the homicide.[8] The defendant was indicted on a charge of murder in the first degree, G. L. c. 265, § 1; attempted masked armed robbery, G. L. c. 274, § 6; five counts of masked armed robbery, G. L. c. 265, § 17; and six counts of unlawful possession of a firearm, G. L. c. 269, § 10 (a). He moved to suppress all of the evidence obtained as a result of the tower dumps, on the ground that it was the fruit of an unconstitutional search.

Following a nonevidentiary hearing, a Superior Court judge denied the motion. The judge concluded that the defendant had a reasonable expectation of privacy in his CSLI, and therefore had standing to challenge the purported search. Nonetheless, because the search warrants had been supported by probable cause, the judge decided that the CSLI, and the evidence subsequently derived from it, had been obtained lawfully. The judge found that both search warrants were sufficiently particular and limited in scope, and rejected the defendant's argument that they amounted to "overbroad, unparticularized general warrants." The defendant then sought leave to pursue an

[8] After having obtained the first warrant, but before applying for the second warrant, the Commonwealth decided that it could not "definitively" determine that the perpetrator who carried out the other offenses was responsible for the robbery on September 28, 2018.

interlocutory appeal in the county court. A single justice of this court allowed the application and reserved and reported the matter to the full court.

2. Discussion. a. Standard of review. Ordinarily, "[i]n reviewing a decision on a motion to suppress, 'we accept the judge's subsidiary findings of fact absent clear error but conduct an independent review of [the] ultimate findings and conclusions of law" (quotation omitted). Commonwealth v. Ramos, 470 Mass. 740, 742 (2015), quoting Commonwealth v. Colon, 449 Mass. 207, 214, cert. denied, 552 U.S. 1079 (2007). Where, as here, the judge's findings are based exclusively on documentary evidence, we review the judge's findings of fact, as well as his or her conclusions of law, de novo. See Commonwealth v. Johnson, 481 Mass. 710, 714, cert. denied, 140 S. Ct. 247 (2019).

b. Whether a search occurred. i. Legal standards. The Fourth Amendment to the United States Constitution and art. 14 protect the right to be free from unreasonable searches.[9] See

[9] State constitutional rules "do[] not constrain Federal authorities unless they operate as part of an 'essentially' State investigation." Commonwealth v. Brown, 456 Mass. 708, 713 (2010), S.C., 466 Mass. 1007 (2013). An investigation is essentially a State investigation where, for example, the purpose of the investigation was to bring State charges, State officials retained significant authority over the investigation, or the State's involvement was otherwise so substantial that it "negate[d] the essentially Federal nature of the investigation." Commonwealth v. Gonzalez, 426 Mass. 313, 317-318 (1997). The

Commonwealth v. Feliz, 486 Mass. 510, 514 (2020). Of course, for those protections to be applicable, "the Commonwealth's conduct must constitute a search in the constitutional sense." See Johnson, 481 Mass. at 715. Such a search occurs "when the government's conduct intrudes on a person's reasonable expectation of privacy."[10] Augustine I, 467 Mass. at 241. "An individual has a reasonable expectation of privacy where (i) the individual has 'manifested a subjective expectation of privacy in the object of the search,' and (ii) 'society is willing to recognize that expectation as reasonable.'" Johnson, supra, quoting Augustine I, supra at 242.

In applying this test to technological surveillance, we must be careful to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." Carpenter, 138 S. Ct. at 2214, quoting Kyllo v. United States, 533 U.S. 27, 34 (2001). In practice, doing so is anything but a simple exercise; advancements in

---

Commonwealth does not dispute that the investigation in this case was essentially a State investigation. Accordingly, the Federal agents involved in the investigation were constrained by the State Constitution. See Commonwealth v. Jarabek, 384 Mass. 293, 297 (1981).

[10] Because the defendant does not contend that the government "physically intrud[ed] on a constitutionally protected area," we do not consider whether a physical search occurred. See Commonwealth v. Johnson, 481 Mass. 710, 715, cert. denied, 140 S. Ct. 247 (2019), quoting Grady v. North Carolina, 575 U.S. 306, 309 (2015).

technology have resulted in a quantity and quality of surveillance that never could have been imagined, let alone realized, at the time of the founding. See United States v. Jones, 565 U.S. 400, 420 (2012) (Alito, J., concurring in the judgment). Thus, while we have "acknowledged the usefulness of these tools in crime detection," we also have "caution[ed] against allowing the 'power of technology to shrink the realm of guaranteed privacy.'" Commonwealth v. Henley, 488 Mass. 95, 109 (2021). See Commonwealth v. Blood, 400 Mass. 61, 69 (1987), quoting Lopez v. United States, 373 U.S. 427, 469 (1963) (Brennan, J., dissenting) ("[i]t must be plain that electronic surveillance imports a peculiarly severe danger to the liberties of the person").

To this end, where police use technology to engage in long-term surveillance, we have analyzed their actions in the aggregate. We first did so with respect to CSLI in Augustine I, 467 Mass. at 253. There, we held that the government effectuated a search when it used targeted CSLI to obtain a list of every cell site to which the defendant's cellular telephone had connected over a two-week period. Id. at 254-255. In so holding, we considered the "cumulative nature of the information collected"; that is, rather than evaluating whether the defendant had a reasonable expectation of privacy in each isolated cell site connection, we evaluated whether the

defendant had such a reasonable expectation in the two weeks of CSLI as a whole. Id. at 253-255.

The aggregation principle we used in Augustine I developed into what is now known as the mosaic theory. See Commonwealth v. McCarthy, 484 Mass. 493, 503 (2020). "The mosaic theory requires that we consider the governmental action as a whole and evaluate the collected data when aggregated." Henley, 488 Mass. at 109. Thus, rather than "asking if a particular act is a search, the mosaic theory asks whether a series of acts that [may not be] searches in isolation amount to a search when considered as a group." Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 (2012). Because "the whole reveals far more than the sum of the parts," a series of acts may be a search even where each step in isolation is not. McCarthy, supra at 504. See District of Columbia v. Wesby, 138 S. Ct. 577, 588 (2018). "As the analogy goes, the color of a single stone depicts little, but by stepping back one can see a complete mosaic." McCarthy, supra. See United States v. Tuggle, 4 F.4th 505, 517 (7th Cir. 2021), cert. denied, 142 S. Ct. 1107 (2022), quoting Kugler & Strahilevitz, Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory, 2015 Sup. Ct. Rev. 205, 205 (2015) ("the mosaic theory attempts to capture the idea that the 'government can

learn more from a given slice of information if it can put that information in the context of a broader pattern, a mosaic'").

In determining whether a series of acts constitutes a search under the mosaic theory, courts have considered "whether the surveillance was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life." Commonwealth v. Mora, 485 Mass. 360, 373 (2020). See Carpenter, 138 S. Ct. at 2217-2218 ("Mapping a cell phone's location [using targeted CSLI] over the course of 127 days" constituted search because it revealed "an intimate window into a person's life" that could not be obtained using traditional surveillance); United States v. Wilford, 961 F. Supp. 2d 740, 771 (D. Md. 2013), aff'd, 689 Fed. Appx. 727 (4th Cir. 2017), cert. denied, 138 S. Ct. 2707 (2018), quoting United States v. Graham, 846 F. Supp. 2d 384, 401-403 (D. Md. 2012), aff'd, 824 F.3d 421 (4th Cir. 2016), cert. denied, 138 S. Ct. 2700 (2018) (mosaic theory turns on whether "discrete acts of surveillance . . . in the aggregate . . . 'paint an "intimate picture"' of a defendant's life").

To answer this question, our limited precedent to date primarily has focused on three general concerns: the extent to which the surveillance reveals the whole of an individual's public movements; the character of the information obtained; and whether the surveillance could have been achieved using

traditional law enforcement techniques. See Henley, 488 Mass. at 113; Mora, 485 Mass. at 373-374; McCarthy, 484 Mass. at 506, 508-509; Augustine I, 467 Mass. at 248, 253. The same concerns have animated the Federal cases that have addressed the issue. See Carpenter, 138 S. Ct. at 2217-2218 (targeted CSLI provides "an all-encompassing record of the holder's whereabouts" and therefore reveals "an intimate window into a person's life" that could not have been obtained under traditional surveillance). See, e.g., United States v. Trice, 966 F.3d 506, 518 (6th Cir. 2020), cert. denied, 141 S. Ct. 1395 (2021), quoting Carpenter, supra (in evaluating duration of surveillance, considering whether it "provided law enforcement with information that was 'otherwise unknowable,'" and "provided an 'intimate window into a person's life'"). See also Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 342-343 (4th Cir. 2021) (electronic aerial surveillance violates reasonable expectation of privacy because it "yield[s] 'a wealth of detail'" that "surpassed ordinary expectations of law enforcement's capacity and provided enough information to deduce details from the whole of individuals' movements" [citation omitted]); State v. Jones, 2017 S.D. 59, ¶¶ 29, 31, 36, cert. denied, 138 S. Ct. 1011 (2018) (search occurred where surveillance that "allowed law enforcement to enhance their senses" revealed "the aggregate of all of [the defendant's] coming and going from the home," thus

providing investigators with "a mosaic of intimate details of [the defendant's] private life and associations").

Whether surveillance reveals the whole of a defendant's movements turns on the duration of the surveillance, as well as its degree of comprehensiveness. See, e.g., Augustine I, 467 Mass. at 254. Long-term surveillance raises particular concerns because it uncovers "types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble," United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), aff'd, 564 U.S. 1036 (2011), thus providing "an intimate window into a person's life" as it existed throughout the duration of the surveillance, Carpenter, 138 S. Ct. at 2217. Such a pattern of activity is far more revealing than details from isolated incidents. See Mora, 485 Mass. at 375-376. "The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life . . . ." Maynard, supra. By way of illustration, a single trip to the liquor store reveals little about an individual, but daily trips over the course of a month reveal much more.

A record is considered to be comprehensive if it has sufficiently voluminous and detailed information from which investigators can derive a relatively complete picture of an

individual's "comings and goings" over time, even if there are gaps in the record. See Carpenter, 138 S. Ct. at 2219. For example, in Augustine I, 467 Mass. at 254-255, we determined that the defendant had a reasonable expectation of privacy in the whole of his public movements, as revealed by targeted CSLI from a single cellular telephone that had accompanied him during a two-week trip, despite the fact that his location was only revealed when he made or received a telephone call. See Jones, 565 U.S. at 404 (electronic tracking of particular vehicle's location provided investigators with whole of defendant's movements, even though tracking only revealed defendant's location while in vehicle); Leaders of a Beautiful Struggle, 2 F.4th at 342-343 (rejecting argument that "gaps in the data" nullified reasonable expectation of privacy in public movements). Even where a record does not include each and every one of a defendant's movements, "the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores

that make up that person's hitherto private routine." McCarthy, 484 Mass. at 504, quoting Maynard, 615 F.3d at 560.

We also have considered the extent to which the surveillance, even if less comprehensive, tended to reveal highly intimate or personal details. See, e.g., Mora, 485 Mass. at 370-372. Because "art. 14 protects against warrantless intrusion into private places," we have expressed particular concern over surveillance that reveals individuals in private settings. See, e.g., Augustine I, 467 Mass. at 253 ("we cannot ignore the probability that, as CSLI becomes more precise, cellular telephone users will be tracked in constitutionally protected areas"). Such surveillance permits investigators to infer whether and when an individual is in constitutionally sensitive areas, such as the home or a place of worship. See Commonwealth v. Yusuf, 488 Mass. 379, 386 (2021), quoting Caniglia v. Strom, 141 S. Ct. 1596, 1599 (2021) ("The very core of [the constitutional] guarantee is the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion" [alterations in original]). Once investigators obtain such information, they are able to piece 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 -- and the pattern of our professional and avocational pursuits.'"

McCarthy, 484 Mass. at 504-505, quoting Commonwealth v. Connolly, 454 Mass. 808, 834 (2009) (Gants, J., concurring), cert. denied, 574 U.S. 1085 (2015).

This information is private and personal even when anonymized, but it provides a much richer profile of an individual if it is linked to his or her identity. See United States Dep't of State v. Ray, 502 U.S. 164, 176 (1991) ("Although disclosure of [certain] personal information constitutes only a de minimis invasion of privacy when the identities of the [individuals] are unknown, the invasion of privacy becomes significant when the personal information is linked to particular [individuals]"). There is, after all, a significant difference between knowing that an anonymized somebody was at a specific political rally and knowing that "John Smith" was at that rally. See Globe Newspaper Co. v. Boston Retirement Bd., 388 Mass. 427, 435 n.14 (1983) (anonymized information "which did not allow the identification of any individual" was not "of a personal nature").

Providing law enforcement with such personal information is of particular concern because it risks chilling the associational and expressive freedoms that our State and Federal Constitutions strive to protect. See Jones, 565 U.S. at 416 (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms");

United States v. Moore-Bush, 381 F. Supp. 3d 139, 148 (D. Mass. 2019) (long-term surveillance "risks chilling core First Amendment activities"). Privacy in one's associations, whether political, religious, or simply amicable, plays a crucial role in maintaining our democracy, and therefore is protected under art. 14. See, e.g., National Ass'n for the Advancement of Colored People v. Alabama, 357 U.S. 449, 462 (1958) (recognizing "the vital relationship between freedom to associate and privacy in one's associations"); Blood, 400 Mass. at 69 (art. 14 protects "the right to be known to others and to know them, and thus to be whole as a free member of a free society").

We also have considered whether the electronic surveillance generated a category or quantity of information that could not have been obtained using traditional law enforcement tools. See, e.g., McCarthy, 484 Mass. at 500. To this end, we have examined whether the surveillance allowed the government to "track and reconstruct a person's past movements, a category of information that never would be available through the use of traditional law enforcement tools of investigation" (emphasis in original). See Augustine I, 467 Mass. at 254. Even where the surveillance at issue theoretically could have been accomplished using traditional surveillance methods, we have taken into account whether those methods would have been prohibitively expensive or otherwise impracticable. See, e.g., McCarthy,

supra at 499-500, quoting Jones, 565 U.S. at 429 (Alito, J., concurring) ("[I]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken"). Because "[h]umans are imperfect note-takers and not all blessed with photographic memory," traditional surveillance often cannot achieve the same level of volume, detail, and precision as electronic surveillance. Moore-Bush, 381 F. Supp. 3d at 149. Moreover, as it is "unlikely that investigators could . . . maintain[] in-person observation over the course of multiple months without [their targets] becoming aware of their presence," technological surveillance that proceeds surreptitiously empowers investigators to engage in long-term, secret surveillance that would not otherwise be possible. See Mora, 485 Mass. at 374.

While these factors have emerged as preeminent in the few cases in which we have applied the mosaic theory to date, we emphasize that the question whether electronic surveillance exposes otherwise unknowable details of a person's life must be answered in light of the totality of the circumstances in each case. Accordingly, these factors are not exhaustive, and no one factor is determinative. A few examples are illustrative.

In McCarthy, 484 Mass. at 508-509, for instance, we decided that police did not intrude on a defendant's reasonable expectation of privacy where they used information obtained from four automatic license plate readers (ALPRs),[11] in fixed positions on either side of two bridges, to determine when, over a period of months, a defendant crossed the bridges. We recognized that the ALPRs provided police with surveillance capabilities that exceeded what would have been possible using traditional law enforcement techniques, but nonetheless reasoned that the limited number of ALPRs, positioned on public highways leading to and from the Cape Cod peninsula, did not "allow the Commonwealth to monitor the whole of the defendant's public movements" or otherwise "reveal 'the privacies of life.'" Id. at 509, quoting Carpenter, 138 S. Ct. at 2217. We noted, however, that even a limited number of ALPRs located near "constitutionally sensitive locations," such as the home or a place of worship, could intrude upon a reasonable expectation of privacy because they "reveal more of an individual's life and associations." McCarthy, supra at 506.

[11] "Automatic license plate readers are cameras combined with software that allows them to identify and 'read' license plates on passing vehicles. When an ALPR identifies a license plate, it records a photograph of the plate, the system's interpretation of the license plate number, and other data, such as the date, time, location, direction of travel, and travel lane." Commonwealth v. McCarthy, 484 Mass. 493, 494 (2020).

Thus, where surveillance falls short of revealing the whole of an individual's movements, it nonetheless may constitute a search when it reveals highly intimate details that practically would not have been obtainable using traditional surveillance. See Mora, 485 Mass. at 369. In Mora, supra at 375-376, we decided that police had effectuated a search by installing and monitoring two pole cameras pointed at the defendants' residences. The cameras revealed when the defendants were at home, when they received visitors, and who those visitors were, and therefore did not reveal the whole of the defendants' movements. See id. at 371-372. Nonetheless, we concluded that the cameras intruded upon the defendants' reasonable expectations of privacy because the information revealed by the surveillance provided investigators with highly intimate details of the defendants' lives that could not have been obtained using traditional surveillance methods. See id. at 374, quoting Jones, 565 U.S. at 420 n.3 (Alito, J., concurring) ("replicating pole camera surveillance 'would have required either a very large [pole], a very tiny constable, or both'").

ii. Application. Here, we must determine whether the government's actions with respect to the seven tower dumps, in the aggregate, intruded upon the defendant's reasonable expectation of privacy by providing investigators with otherwise

unknowable details of life.[12] We begin by aggregating the several actions investigators took in acquiring and analyzing the defendant's CSLI. See Henley, 488 Mass. at 113. Investigators first obtained seven tower dumps, spanning seven different days over the course of slightly more than one month; each tower dump was limited in time to the period immediately before and after the specific robbery for which the CSLI was sought. Investigators then cross-referenced the information obtained from the tower dumps to isolate particular telephone numbers that appeared at more than one location. Thereafter, investigators analyzed the CSLI associated with those telephone numbers, among them the defendant's telephone number, to determine (1) the approximate location of the connecting cellular telephone, (2) the identity of the telephone's user, and (3) the identity of the person with whom the user was communicating.

These actions, viewed in their entirety, provided investigators with information of a highly personal and private

---

[12] The Commonwealth does not dispute that the defendant manifested a subjective expectation of privacy in his CSLI records. The defendant submitted an affidavit averring that he never affirmatively permitted law enforcement officers to access his CSLI. See Augustine I, 467 Mass. at 255 & n.38 (subjective expectation of privacy was satisfied where defendant averred that he "never permit[ed] the police or other law enforcement officials access to his telephone records"). Accordingly, we focus on the reasonableness of the defendant's subjective expectation.

nature. Because tower dumps locate individuals when they are in private settings just as easily as when they are in public settings, they have "the potential to track a cellular telephone user's location in constitutionally protected areas." Augustine I, 467 Mass. at 249. Moreover, tower dumps enable investigators to infer the identity of the individual with whom the user of a particular device was communicating at the moment the device connected to the cell site, and therefore provide investigators with significant insight into the individual's associations.

An owner's location and associations are tied to his or her telephone number and unique identifier, which, here, were used to discern the defendant's identity and that of his suspected accomplice. Moreover, because investigators obtained seven tower dumps spanning seven distinct dates over the course of more than one month, they also were able to piece together a pattern of behavior, that is, not only where an individual was and with whom he or she associated on one occasion, but also where the individual had been and with whom the individual had associated on multiple different occasions.

The collective whole of this personal and private information would have been impossible to obtain through the use of traditional surveillance techniques. The government learned the defendant's comings and goings during a period of time

before he was a suspect, something that could not have been achieved through visual surveillance. See Augustine I, 467 Mass. at 254. Indeed, the sheer volume of information investigators obtained from the tower dumps would have been impossible to gather using traditional surveillance. See id. There is no historic analogue for the ability effortlessly to compile and document the locations, identities, and associations of tens of thousands of individuals, just in case one might be implicated in a criminal act.[13] Even if such a feat were possible, it certainly would be impossible to execute surreptitiously; yet, here, investigators were able to compile and catalogue the locations of more than 50,000 individuals at varying points over more than one month, without any one of them ever knowing that he or she was the target of police surveillance.

In light of these factors, and in the totality of the circumstances, the collection and subsequent analysis of the seven tower dumps at issue here provided investigators with

[13] Traffic cameras might provide the closest analogue, insofar as they can reveal the retrospective location of potentially a substantial number of people. Traffic cameras, however, only locate a person in public areas, whereas tower dumps provide information about public and private locations. Moreover, while traffic cameras may reveal an individual's physical features, tower dumps enable investigators to determine a person's precise identity using his or her telephone number or unique identifier.

highly personal and previously unknowable details of the defendant's life. Accordingly, the Commonwealth's use of the seven tower dumps intruded upon the defendant's reasonable expectation of privacy.

The Commonwealth contends that the government's actions here should not be considered a search because the seven tower dumps only produced, in total, three hours of CSLI. In support of its position, the Commonwealth points to Commonwealth v. Estabrook, 472 Mass. 852, 858 (2015), where the court held that no search takes place when police obtain six or fewer hours of targeted CSLI, giving them a list of each cell site with which an identified cellular telephone has connected during that period. We reasoned that, although government collection and use of targeted CSLI over a longer period of time intrudes upon an individual's reasonable expectation of privacy, location information covering six hours or less is too brief in duration to do so. Id.

While Estabrook, 472 Mass. at 855, involved targeted CSLI, its reasoning also is applicable to tower dumps. Given that tower dumps reveal an individual's locations at discrete moments in time, the individual privacy interests implicated by tower dumps are akin to those implicated by targeted CSLI.[14] Compare

[14] The defendant argues that there is a heightened privacy interest in the context of tower dumps because they provide CSLI

McCarthy, 484 Mass. at 509 (no reasonable expectation of privacy in location of individual's vehicle, as revealed by limited number of cameras in particular public location, at specific point in time), with Commonwealth v. Rousseau, 465 Mass. 372, 382 (2013) (reasonable expectation of privacy in entirety of vehicle's movements over thirty-one days). The court's holding in Estabrook, supra at 858, is inapplicable here; the holding permits a warrantless search of up to six continuous hours of CSLI, where, here, the government obtained small increments of CSLI, each falling on a separate day. The rationale in Estabrook was that analyzing six hours or less of telephone call CSLI could not be a search "because the duration is too brief to implicate the person's reasonable privacy interest." See id., quoting Augustine I, 467 Mass. at 254. While the court has determined that analyzing six continuous hours of CSLI does not intrude upon a reasonable expectation of privacy, analyzing small increments of CSLI over the course of several days does. Whereas the former reveals at most one-quarter of one day's

---

on "potentially thousands of innocent persons." The rights secured by art. 14, however, "are specific to the individual." Commonwealth v. Delgado-Rivera, 487 Mass. 551, 554 (2021), cert. denied, 142 S. Ct. 908 (2022). Thus, in determining whether a search occurred, we focus exclusively on the defendant's privacy interests, and cannot consider the privacy interests of others. See id. at 556, 564 (defendant could not rely on codefendant's reasonable expectation of privacy in cellular telephone in establishing that search occurred).

activities, the latter reveals a pattern of activity, which implicates comparatively greater privacy interests. See Mora, 485 Mass. at 375-376. Accordingly, although Estabrook, supra, enables the Commonwealth to obtain one or more tower dumps spanning six hours or less without a warrant, it provides no refuge where, as here, the tower dumps span multiple days.

c. Whether the Commonwealth's acquisition of the tower dumps was constitutionally infirm. Because the Commonwealth's actions constituted a search, we must determine whether its conduct in effectuating that search was reasonable.

Article 14 "require[s] that all searches and seizures be reasonable." Commonwealth v. Alexis, 481 Mass. 91, 97 (2018). "Searches and seizures conducted outside the scope of a valid warrant are presumed to be unreasonable," and therefore unconstitutional. Commonwealth v. Balicki, 436 Mass. 1, 8 (2002). "To be reasonable in the constitutional sense," a search conducted pursuant to a warrant must be supported by probable cause. Commonwealth v. Neilson, 423 Mass. 75, 77 (1996). To comport with constitutional protections, an affidavit in support of a search warrant for CSLI must demonstrate "probable cause to believe [1] 'that a particularly described offense has been, is being, or is about to be committed, and [2] that [the CSLI being sought] will produce evidence of such offense or will aid in the apprehension of a

person who the applicant has probable cause to believe has committed, is committing, or is about to commit such offense'" (alterations in original). Estabrook, 472 Mass. at 870, quoting Augustine I, 467 Mass. at 256. Accordingly, the warrant affidavit must show "a sufficient nexus between the criminal activity for which probable cause has been established and the physical location of the cell phone recorded by the CSLI." Commonwealth v. Hobbs, 482 Mass. 538, 547 (2019). A nexus is sufficient where "the information available to police 'provide[s] a substantial basis for concluding that evidence connected to the crime will be found [in] the [location to be searched]." See Commonwealth v. Ortiz, 487 Mass. 602, 606 (2021), quoting Commonwealth v. Escalera, 462 Mass. 636, 642 (2012).

i. Probable cause. The defendant argues that the search of the CSLI here was unlawful because neither supporting affidavit established probable cause. Specifically, he maintains that the search warrant affidavits did not demonstrate a nexus between the commission of the offenses and the CSLI to be searched, as the affidavits did not set forth particularized evidence that the perpetrator had used a cellular telephone during the commission of the offenses, or in the periods immediately before or thereafter. Relying on Commonwealth v. Morin, 478 Mass. 415, 426 (2017), the defendant contends that

the only statements in the affidavits demonstrating that the perpetrator "possessed a phone during the robberies" were general conclusions about the ubiquity of cellular telephones, which cannot be used to establish probable cause.[15] See id. (in demonstrating existence of probable cause to search contents of cellular telephone, "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").

As the defendant contends, to establish probable cause to search the contents of a cellular telephone, "it is not enough that the object of the search may be found in the place subject to search. . . . Rather, the affidavit must demonstrate that . . . the items sought will be located in the particular data file . . . to be searched" (emphasis in original). Commonwealth v. Broom, 474 Mass. 486, 496 (2016). General statements concerning the ubiquity of cellular telephones are

[15] The affidavit in support of the second warrant stated that "[s]mart phone/electronic device utilization is one of the most common activities today and the vast majority of American society bring their device [wherever] they go, almost by habit." Similarly, the affidavit in support of the first warrant stated that "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."

insufficient to establish the required nexus. See Morin, 478 Mass. at 426. This "more narrow and demanding standard," however, is applicable to searches of cellular telephones and computer-like devices, see Hobbs, 482 Mass. at 547 n.11, quoting Commonwealth v. Holley, 478 Mass. 508, 524 (2017), and not to searches of CSLI. While a search of the contents of a cellular telephone permits police to view "vast amounts of sensitive and private data," the "same concerns are not present in the context of CSLI, where the cell phone's location, and not its contents, is sought." Hobbs, supra. Thus, when seeking a warrant to search CSLI, investigators need not establish "that the defendant actually used or possessed his [or her] cell phone during the commission of the crimes" (emphasis added), which they would be required to do in order to search its contents. See id. at 546. Rather, the nexus requirement is satisfied as long as there is a substantial basis to conclude that the defendant used his or her cellular telephone during the relevant time frame, such that there is probable cause to believe the sought after CSLI will produce evidence of the crime. See id.

Here, it is undisputed that the Commonwealth established probable cause to believe that the offenses described in the warrant had been committed. Accordingly, we consider whether each warrant affidavit established a substantial basis to believe that a search of the requested tower dumps would produce

evidence of the crimes under investigation, or would aid in the apprehension of the perpetrator. See Estabrook, 472 Mass. at 870. Because the probable cause analysis is "fact-intensive and [must] be resolved on a case-by-case basis," we review each warrant application separately. See Commonwealth v. Vasquez, 482 Mass. 850, 867 (2019), S.C., 485 Mass. 405 (2020), cert. denied, 141 S. Ct. 2601 (2021). We begin with the second warrant, in which the warrant affidavit discussed all of the offenses under investigation in depth, before considering the less-detailed first warrant.[16]

A. Second warrant. The second search warrant affidavit described several notable similarities between the offenses. Each robbery, as well as the attempted robbery, was committed against a clerk at a store, almost always a convenience store, in or around Boston, sometime during the period between dusk and dark. The perpetrator always brandished a black semiautomatic pistol, which he held in his right hand. Witnesses consistently described the perpetrator as a light-skinned Black or Hispanic male, approximately six feet, two inches tall, with a medium to thin build, dressed in a black hooded jacket, dark-colored

[16] The affidavit in support of the second warrant did not rely on any evidence obtained pursuant to the first warrant. Accordingly, suppression of the evidence from the first warrant would have no bearing on the admissibility of the evidence obtained pursuant to the second warrant. See Commonwealth v. Tyree, 455 Mass. 676, 692 (2010).

pants, black gloves, black shoes, and a black or red mask. In addition, on two occasions, surveillance footage showed a hole or a light-colored blemish on the robber's jacket. Collectively, this evidence provided a substantial basis to believe, see Escalera, 462 Mass. at 642, that the same individual had committed all of the offenses, see Commonwealth v. Marrero, 427 Mass. 65, 71-72 (1998), quoting Commonwealth v. Cordle, 404 Mass. 733, 740 (1989), S.C., 412 Mass. 172 (1992) ("Although the circumstances of the . . . offenses were not identical, we think they were sufficiently similar to justify the inference that they were the product of the same mind" [alterations in original]).

The second warrant affidavit also described evidence indicating that a suspected coventurer had acted as a getaway driver in at least three of the offenses under investigation. The robberies took place from two to eleven miles apart, and some of the locations were not near any public transportation. On October 4, 2018, the store clerk saw the perpetrator enter the passenger's side of a dark-colored sedan, without removing his mask, before quickly departing the scene. On October 6, 2018, a surveillance camera recorded video footage of a dark-colored sedan or coupe traveling at a high rate of speed along the perpetrator's path of flight, as recorded by a separate surveillance camera. Moreover, on October 31, 2018, police

canines detected the perpetrator's scent along his reported flight path, but the scent ended abruptly in a public area with no nearby public transportation, which could have indicated that the perpetrator entered a vehicle. See Wilkerson, 486 Mass. at 172 (considering existence of and coordination with coventurer in finding probable cause to obtain CSLI).

The search warrant affidavit also described facts suggesting some reason to believe that the defendant and a coventurer had communicated with one another from a distance, either prior to or after the commission of the offense. The detective seeking the search warrant averred that, based on his experience and training, violent crimes such as those at issue often require some level of coordination amongst coventurers. See Holley, 478 Mass. at 522 (statement that particular crime often involves coordination among codefendants by cellular telephone was considered as one factor in probable cause analysis). This coordination could have taken place while the perpetrators were apart; the robber appeared to travel some distance on foot prior to or after most of the robberies, and therefore was at least temporarily separated from the getaway driver. The evidence that the perpetrator and the coventurer communicated from a distance, when combined with the affiant's statements about the over-all ubiquity of cellular telephones, provided reasonable grounds to believe that the robber and the

getaway driver had used cellular telephones to communicate. See Commonwealth v. Almonor, 482 Mass. 35, 45 (2019), quoting Augustine I, 467 Mass. at 245-246 (cellular telephones "exist as 'almost permanent attachments to [their users'] bodies'" and "physically accompany their users everywhere").

Because there was reason to believe that the perpetrator used a cellular telephone to communicate with a coventurer around the time of the offenses, there also was probable cause to believe that either the perpetrator's telephone or the coventurer's telephone would have produced telephone call CSLI that would appear in the requested tower dumps, and likely in more than one of the tower dumps. This CSLI, in turn, would enable investigators to isolate potential suspects by determining which, if any, individuals had been near the scene of two or more of the offenses. See Hobbs, 482 Mass. at 546 (location of cellular telephone as recorded by CSLI can be "reasonably expected to be the location of the person possessing the cell phone"). Accordingly, the second warrant affidavit was supported by probable cause.

B. First warrant. The affidavit in support of the first warrant, much like the affidavit in support of the second warrant, outlined significant similarities amongst the offenses then under investigation, and therefore afforded a substantial basis to believe that the offenses had been committed by the

same individual. Additionally, the affidavit demonstrated reason to believe that the perpetrator had been, at least occasionally, assisted by a coventurer.

The first warrant affidavit did not, however, set forth any particularized information that the perpetrator or the coventurer owned a cellular telephone or communicated with one another from a distance. Compare Commonwealth v. Louis, 487 Mass. 759, 765 (2021) (evidence showed that suspect "communicated with another robbery suspect via cell phone on the date of the murder"); Hobbs, 482 Mass. at 547 (affidavit for targeted CSLI must show that "suspect was known to own or use a particular cell phone"). Moreover, the first warrant affidavit did not discuss the need for coventurers to communicate when committing a robbery, nor did it point to any evidence that the perpetrator and the coventurer had been separated during the commission of the crime such that they would have had to communicate from a distance.

Thus, the only ground in the first affidavit upon which to conclude that the perpetrator had possessed or used a cellular telephone to aid in accomplishing the crimes was the affiant officer's statement that "it is very common for a person to have a cellular telephone with them at all times." See Commonwealth v. Rosetti, 349 Mass. 626, 632 (1965) (probable cause must be based on particularized facts, not "simply general

conclusions"). Therefore, the evidence obtained pursuant to the first warrant must be suppressed. See Commonwealth v. Andre, 484 Mass. 403, 408 (2020).

ii. Particularity.[17] The defendant also argues that the search here was unreasonable because the search warrants themselves lacked particularity, and therefore were unconstitutional general warrants. He maintains that, if the search of the CSLI was a search in the constitutional sense with respect to him, it necessarily follows that everyone whose CSLI was contained in the tower dumps also was searched. This would render the warrants unconstitutional general warrants because they permitted law enforcement to search the CSLI of third parties who merely were present in the vicinities of the offenses being investigated, without any probable cause. In the defendant's view, the only way to ensure that the scope of a search is sufficiently narrow is to require warrants for CSLI to identify the targeted suspect by name or telephone number.

As the defendant emphasizes, art. 14 "require[s] that a search warrant describe with particularity the places to be searched and the items to be seized." Commonwealth v. Perkins, 478 Mass. 97, 106 (2017). The particularity requirement "both

[17] Having concluded that the first warrant was not supported by probable cause, we need not consider whether it lacked particularity.

defines and limits the scope of the search and seizure." Commonwealth v. Pope, 354 Mass. 625, 629 (1968). "The dual purposes of the particularity requirement are '(1) to protect individuals from general searches and (2) to provide the Commonwealth the opportunity to demonstrate, to a reviewing court, that the scope of the officers' authority to search was properly limited.'" Holley, 478 Mass. at 524, quoting Commonwealth v. Valerio, 449 Mass. 562, 566-567 (2007). See Riley v. California, 573 U.S. 373, 403 (2014) (general searches "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity"). To this end, a warrant must describe the object of the search with enough specificity that investigators can identify, with reasonable certainty, that which they are authorized to search, thus ensuring that they search only those items for which probable cause exists. See Commonwealth v. Treadwell, 402 Mass. 355, 359 (1988).

The precise degree of particularity required "necessarily var[ies] according to the circumstances and the type of items involved." See Commonwealth v. Freiberg, 405 Mass. 282, 298, cert. denied, 493 U.S. 940 (1989), quoting United States v. Johnson, 541 F.2d 1311, 1314 (8th Cir. 1976). More generality may be tolerated where a more precise description would be impracticable. See, e.g., Henley, 488 Mass. at 119 (warrant for

search of contents of cellular telephone need not particularly identify specific electronic file to be searched "where officers had no knowledge of where on the cell phone evidence might be located, or in what format, but specifically identified the type of evidence sought"); Commonwealth v. McDermott, 448 Mass. 750, 775, cert. denied, 552 U.S. 910 (2007) (warrant permitting search of computer files relating to defendant's mental health did not lack particularity because "[t]he lack of further specificity was practical in the circumstances, and the mental health category was limited as much as possible in the circumstances").

We do not agree that all of the individuals whose CSLI was revealed by the tower dumps were subjected to a search in the constitutional sense. The defendant's reasonable expectation of privacy was invaded not simply by law enforcement's possession of his anonymized CSLI, but also by the investigating officers' possession and analysis of that CSLI, the aggregate of which provided investigators with a revealing mosaic of the defendant's private life. See Henley, 488 Mass. at 109 (search inquiry under mosaic theory focuses on "the governmental action as a whole"). See also Kerr, supra at 320 (search occurs where government "collection and subsequent analysis" of data reveals mosaic [emphasis added]). A cursory examination of anonymized CSLI would not permit investigators to infer the identity of any

given individual, where within the cell site's radius that person had been, or with whom he or she had associated; thus, such an examination would not intrude upon a reasonable expectation of privacy. See Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976); McCarthy, 484 Mass. at 504. Only those individuals whose CSLI was subject to further analysis -- such as the defendant -- were subject to a search within the meaning of art. 14. The question, then, becomes whether the second warrant sufficiently limited the set of telephone numbers and their associated CSLI that investigating officers were permitted to analyze, and therefore to search.

As the defendant maintains, the scope of the search authorized by the warrant, on its face, is not entirely clear. Under "property to be searched," the warrant lists the "records and information associated with the cellular telephone towers/sites ('Cell Towers/Sites') that provided cellular service" in the vicinity of the crimes during the forty-minute period surrounding each offense. With respect to "particular items to be seized," the warrant identifies the categories of information that the service provider must disclose, including, inter alia, the telephone number of the connecting cellular telephone and the sector of the cell site providing service to each connecting telephone. Thus, if read in isolation, the warrant would permit investigators to analyze, without

limitation, any and all CSLI in the tower dumps. Investigators permissibly could select any telephone number from among the 50,000 provided and thereafter conduct a search by determining the identity of that individual, his or her location, and with whom he or she had been communicating, all without even an iota of suspicion. Judicial authorization of such "general exploratory rummaging" undoubtedly would violate the particularity requirements of art. 14. See Balicki, 436 Mass. at 7.

Any deficiencies in the warrant itself, however, were remedied by the supporting affidavit, which adequately limited the scope of the search.[18] See Commonwealth v. Dorelas, 473 Mass. 496, 499 n.3 (2016) (although warrant lacked particularity on its face, search was permissible because affidavit limited scope of search). The supporting affidavit explained that investigators sought to obtain the tower dumps in order "to identify and/or verify commonalities within [the] requested records." Thus, police were permitted to isolate and analyze the CSLI of those telephone numbers that appeared in two or more

[18] A supporting affidavit can remedy a particularity defect in a warrant where (1) the warrant makes "specific reference to the affidavit" and (2) the officer who submitted the affidavit in support of the warrant was "one of the [officers] executing the warrant." See Commonwealth v. Todisco, 363 Mass. 445, 450 (1973). See also E.B. Cypher, Criminal Practice and Procedure § 5:101 (4th ed. 2021).

tower dumps, but no others. Otherwise put, because the warrant authorized the search of only a narrow subset of the CSLI, for purposes of identifying a common suspect, it was sufficiently particular.[19]

As the scope of the search was limited in this manner, that the warrant did not identify a suspect by name or telephone number did not render it insufficiently particular. Unlike an arrest warrant, a search warrant "need not identify a specific criminal suspect -- although frequently it does." Commonwealth v. Martinez, 476 Mass. 410, 419 (2017). See Commonwealth v. Mora, 477 Mass. 399, 404 (2017) ("it is not necessary for the [warrant] application to identify a suspect"). "[S]earch warrants are often employed early in an investigation, perhaps before the identity of any likely criminal and certainly before all the perpetrators are or could be known." Zurcher v. Stanford Daily, 436 U.S. 547, 561 (1978). Requiring police to identify a presently unknown suspect by name "would unreasonably thwart the ability of the police to investigate a crime." See

[19] The scope of the search was further limited because the warrant permitted investigators to obtain data only for brief periods of time (measured in minutes) surrounding the commission of the offenses. See Commonwealth v. Hobbs, 482 Mass. 538, 546, 549 (2019) (duration of search of targeted CSLI must be limited to period of time bearing sufficient nexus to crime under investigation); Commonwealth v. Dorelas, 473 Mass. 496, 503 (2016) (search of electronically stored information must be limited to electronic files where evidence of crime "may reasonably be found").

Freiberg, 405 Mass. at 299. Although limiting a search of CSLI to an identified suspect might be the better practice where possible, it is not required where, as here, the suspect's identity is unknown and the scope of the search is appropriately limited through other means. Compare id. at 299-300 (warrant permitting seizure of "instrument[s] used in crime" was sufficiently particular because "the exact characteristics of [the instruments] were not known to [police]" and warrant affidavit "made it reasonably clear that the 'instrumentalities' sought were related to a crime of violence"), with Commonwealth v. Taylor, 383 Mass. 272, 276 (1981) (warrant was not sufficiently particular where "the particularization was available but was not used in the warrant").

c. Prospective limits on tower dump warrants. General Laws c. 211, § 3, grants this court "general superintendence of the administration of all courts of inferior jurisdiction." Under this authority, we may "impose requirements (by order, rule or opinion) that go beyond constitutional mandates," Commonwealth v. O'Brien, 432 Mass. 578, 584 (2000), quoting Commonwealth v. Bastarache, 382 Mass. 86, 102 (1980), including those governing the issuance and content of warrants, see, e.g., Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 821-822 (2013); Rodriques v. Furtado, 410 Mass. 878, 888 (1991). Although this power "is to be used sparingly," it appropriately

may be exercised "in exceptional circumstances and where necessary to protect substantive rights in the absence of an alternative, effective remedy" (citation omitted). MacDougall v. Commonwealth, 447 Mass. 505, 510 (2006).

While the decision we reach today is grounded in individual rights protected by art. 14, we recognize the potential invasions of privacy that could befall those innocent and uninvolved third parties whose CSLI is revealed once an application for a search warrant is allowed. See generally Owsley, supra at 44. Unlike defendants in criminal cases, these individuals may never know that their CSLI was provided to law enforcement, let alone be able to exercise any sort of control or oversight over how their data is used. See id. at 46. Such a situation presents far too great a risk of unwarranted invasions of privacy, whether intentional or inadvertent, malicious or innocent. Cf. Preventative Med. Assocs., Inc., 465 Mass. at 821-822 (exercise of superintendence power was warranted given risk of irreparable invasion of privacy).

Accordingly, in all future cases, only a judge may issue a search warrant for tower dumps. See id. at 822 ("as an exercise of our supervisory powers, we shall require in all future cases that only a Superior Court judge may issue a search warrant seeking e-mails of a criminal defendant under indictment"); Rodriques, 410 Mass. at 888 ("under the exercise of our general

superintendence powers, we shall deem a warrant authorizing the search of a body cavity to be invalid unless issued by the authority of a judge"); G. L. c. 272, § 99 F 1 ("warrant to intercept wire or oral communications" must be issued by Superior Court judge).

The warrant must include protocols for the prompt and permanent disposal of any and all data that does not fit within the object of the search following the conclusion of the prosecution. See Matter of the Application of the U.S.A. for an Order Pursuant to 18 U.S.C. §§ 2703(c) & 2703(d) Directing AT&T, Spring/Nextel, T-Mobile, Metro PCS & Verizon Wireless to Disclose Cell Tower Log Info., 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014) (warrant application for tower dump must "outline[] a protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved"); Matters of the Search of Cellular Tel. Towers, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) ("the Government is ordered to return any and all original records and copies . . . to the Provider, which are determined to be not relevant to the Investigative Agency's investigation"); Matter of the Application of the U.S.A. for an Order Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Location Records, 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012) (warrant for tower dump must include protocol for handling of "data related to innocent

people who are not the target of the criminal investigation"). See also G. L. c. 276, § 3 ("all property seized [pursuant to a search warrant] shall be restored to the owners thereof" "[a]s soon as may be").

d. Retroactivity. Because we are announcing a constitutionally mandated requirement for the first time, we also must consider whether our holding is to be applied retroactively. The retroactivity of a constitutional rule of criminal procedure turns on whether the rule is "new" or "old." Commonwealth v. Ashford, 486 Mass. 450, 457 (2020). "[A] case announces a new rule if the result was not dictated by precedent" (emphasis in original). Commonwealth v. Bray, 407 Mass. 296, 301 (1990), quoting Teague v. Lane, 489 U.S. 288, 301 (1989). "[A] holding is not so dictated . . . unless it would have been 'apparent to all reasonable jurists.'" Chaidez v. United States, 568 U.S. 342, 347 (2013), quoting Lambrix v. Singletary, 520 U.S. 518, 527-528 (1997).

The rule we announce today undoubtedly is new; we are unaware of any existing statute or prior judicial opinion that would have obligated investigators to obtain a search warrant before acquiring or analyzing tower dumps. See Augustine I, 467 Mass. at 257. Accordingly, our holding applies prospectively and to those cases that are active or pending on direct review

on the date of issuance of the rescript in this case.[20] See Diatchenko v. District Attorney for the Suffolk Dist., 466 Mass. 655, 664 (2013), S.C., 471 Mass. 12 (2015).

3. Conclusion. The Commonwealth's actions in this case intruded upon the defendant's reasonable expectation of privacy and therefore effectuated a search under art. 14. Nonetheless, because the second warrant was sufficiently particular and supported by probable cause, the evidence obtained pursuant to the second warrant need not be suppressed. All evidence stemming from the tower dumps provided pursuant to the first warrant, however, must be suppressed because the warrant was not supported by probable cause. Our decision is prospective, and also applies to those cases that are active or pending on direct review on the date of issuance of the rescript in this case. Henceforth, before acquiring and analyzing a series of tower dumps, the Commonwealth must obtain a warrant from a judge. Before issuing the requested warrant, the judge must ensure that

[20] New rules apply retroactively if the rule "is 'substantive,' defining a class of conduct that cannot be deemed criminal, or prohibiting imposition of a type of punishment on a particular class of defendants" or "establishes a 'watershed' rule of criminal procedure that is 'implicit in the concept of ordered liberty,' implicating the fundamental fairness of the proceeding." Augustine I, 467 Mass. at 257 n.39, quoting Diatchenko v. District Attorney for the Suffolk Dist., 466 Mass. 655, 665 (2013), S.C., 471 Mass. 12 (2015).

it provides a protocol for the disposal of any data that falls outside the scope of the search.

So ordered.