SJC-12750

COMMONWEALTH vs. JASON J. McCARTHY.

Barnstable. October 2, 2019. - April 16, 2020.

Present (Sitting at Barnstable): Gants, C.J., Lenk, Gaziano, Lowy, Budd, Cypher, & Kafker, JJ.

Privacy. Constitutional Law, Privacy, Search and seizure, Standing, Admissions and confessions, Voluntariness of statement. Search and Seizure, Expectation of privacy, Electronic surveillance, Motor vehicle. Practice, Criminal, Motion to suppress, Standing, Admissions and confessions, Voluntariness of statement. Evidence, Admissions and confessions, Voluntariness of statement.

Indictment found and returned in the Superior Court Department on August 31, 2017.

Pretrial motions to suppress evidence were heard by Robert C. Rufo, J.

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

Paul A. Bogosian for the defendant.

Elizabeth A. Sweeney, Assistant District Attorney, for the Commonwealth.

David R. Fox, for Digital Recognition Network, Inc., amicus curiae, submitted a brief.

Matthew Spurlock & David Rassoul Rangaviz, Committee for Public Counsel Services, Ashley Gorski, of New York, Jennifer Lynch & Andrew Crocker, of California, Jessie J. Rossman, Matthew R. Segal, & Nathan Freed Wessler, for American Civil Liberties Union & others, amici curiae, submitted a brief.

GAZIANO, J. While investigating the defendant on suspicion of drug distribution, police used automatic license plate readers (ALPRs) on the Bourne and Sagamore bridges to track his movements. They accessed historical data, which revealed the number of times he had crossed the bridges over a three-month period, and also received real-time alerts, one of which led to his arrest. We must determine whether the use of ALPR technology in this case constituted a search under the Fourth Amendment to the United States Constitution or under art. 14 of the Massachusetts Declaration of Rights.

We conclude that, while the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of ALPRs, that interest is not invaded by the limited extent and use of ALPR data in this case.

1. Background. We draw the following from the facts found by the motion judge, reserving some facts for later discussion.

a. ALPR systems. 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. In Massachusetts, cameras owned and maintained by the State police feed this information into a database maintained by the Executive Office of Public Safety and Security (EOPSS).[1] At some point in 2015, the State police installed fixed camera readers on both sides of the Sagamore and Bourne bridges. While these cameras are not infallible,[2] they essentially create a comprehensive record of vehicles traveling onto or off of the Cape.

ALPR systems produce two related types of information: real-time alerts and historical data. First, individuals with user credentials can log onto the ALPR system, enter license plate numbers onto a "hot list," and choose users to be notified about any new "hits" for that plate number. If a camera in the ALPR system detects a license plate that matches a number on the hot list, the system sends an electronic mail message or text

---

[1] According to the amici, private companies also own and operate automatic license plate reader (ALPR) cameras and share that data with law enforcement, as do individual homeowners. Federal and State law enforcement offices, in turn, may share data with each other.

[2] A testifying expert identified weather conditions, warped or obscured plates, and particularly bad lighting conditions as factors that might result in the ALPR failing to read a particular license plate.

message to the specified officers. Alert recipients receive an image of the plate, along with the date, time, location, and direction of travel. Second, users can search by license plate number for any historical matches stored in the database. EOPSS currently has a one-year retention policy for ALPR data.[3]

The Barnstable police department has adopted the State police general order setting out various regulations for the use of ALPR information. See State police General Order No. TRF-11 (July 22, 2014) (Order TRF-11).[4]

b. The investigation. Through surveillance, several "controlled buys," and information from four confidential informants, the Barnstable police developed substantial evidence that a codefendant in this case was distributing heroin from his residence. During that surveillance, they observed a black Hyundai vehicle appear briefly at the codefendant's residence.

---

[3] Aside from any changes to retention policy or failure to implement purging according to the policy, electronic mail messages sent after a real-time alert may be retained longer than one year, indeed indefinitely, on the recipient's server, as was the case here.

[4] State police General Order No. TRF-11 (July 22, 2014) (Order TRF-11) requires, inter alia, that only trained, specially designated users may access the system; that the "ALPR System and information shall be . . . [a]ccessed and used only for official and legitimate law enforcement purpose"; and that prior to initiating a stop based on an ALPR hit or alert, the officer must verify visually the alphanumeric characters on the license plate and verify the status of the plate through one of various databases.

After further surveillance, and a tip from a confidential informant, police observed the defendant driving the same vehicle, and they began to suspect that he was supplying heroin to his codefendant.

On February 1, 2017, Barnstable police added the license plate number of the black Hyundai to the ALPR hot list, and specified officers to be notified when it was detected crossing the Bourne or Sagamore bridges. On February 8, 2017, several police officers received an alert that the Hyundai had been driven over the Sagamore Bridge onto Cape Cod. Officers subsequently traveled to the codefendant's house and then followed him to Shallow Pond Road in Centerville. At the same time, another officer found the defendant after he drove onto the Cape and followed him to Shallow Pond Road. The officers watched the defendant and the codefendant meet, but no physical exchange was observed. Both vehicles left after approximately thirty seconds.

Police also generated a spreadsheet indicating every time that the Hyundai had passed over the Bourne and Sagamore bridges between December 1, 2016, and February 12, 2017. The spreadsheet contained the dates, times, directions, and specific lanes that the Hyundai had traveled on the bridges. The ALPR spreadsheet showed that the vehicle traveled onto Cape Cod on eight days in February, twenty-one days in January, and nineteen

days in December. On multiple of these days, the defendant made more than one trip on the same day. This appeared consistent with the police theory that the defendant routinely was bringing heroin onto the Cape for distribution by his codefendant.

On February 22, 2017, Barnstable police received another alert that the Hyundai had traveled over the Sagamore Bridge onto Cape Cod. Police again followed both the defendant and the codefendant as they drove to Shallow Pond Road. The officers observed a meeting, but did not see an exchange of objects. Both vehicles departed thirty seconds later. This time, police stopped both vehicles on suspicion that a drug transaction had taken place.

After stopping the codefendant, police handcuffed him, read him his Miranda rights, and questioned him at the side of the road. He made incriminating statements, and officers found heroin on his person. Police also ordered the defendant out of his vehicle, handcuffed him, and read him his Miranda rights. The motion judge found that the defendant was under arrest at the moment that he was ordered out of the Hyundai and handcuffed.

At the police station, the defendant waived his Miranda rights and made various incriminating statements. Officers also seized two cellular telephones and United States currency from the defendant's person. The defendant's brother brought more

money to pay the bail for the defendant, but police seized almost all of the cash on the belief that it was the proceeds of illegal drug activity.

The defendant filed motions to suppress the ALPR data and the fruits of the arrest. A Superior Court judge held an evidentiary hearing and then denied the motions. The defendant then filed an application for leave to pursue an interlocutory appeal in the county court, pursuant to Mass. R. Crim. P. 15 (a) (2), as appearing in 474 Mass. 1501 (2016); the single justice allowed the appeal to proceed in this court.

2. Discussion. "In reviewing a decision on a motion to suppress, we accept the judge's subsidiary findings absent clear error but conduct an independent review of [the] ultimate findings and conclusions of law" (quotations and citation omitted). Commonwealth v. Jones-Pannell, 472 Mass. 429, 431 (2015). Here, reviewing the judge's conclusions of law requires us to determine, among other things, whether the use of ALPR technology by police constitutes a search under the Fourth Amendment or art. 14.

a. ALPRs and constitutional search protections. Under both the Fourth Amendment and art. 14, a search implicates constitutional protections when the government "intrudes on a person's reasonable expectation of privacy" (citation omitted). Commonwealth v. Almonor, 482 Mass. 35, 40 (2019). "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" (quotations and citation omitted).[5] Commonwealth v. Johnson, 481 Mass. 710, 715, cert. denied, 140 S. Ct. 247 (2019). See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

The constitutional jurisprudence governing the technological surveillance of public space has developed rapidly in the last decade. To place the current situation in the proper context, it is necessary to review these developments and their underlying reasoning at some length.

i. Expectations of privacy and technology. As this court and the United States Supreme Court interpret society's reasonable expectations of privacy over time, the courts' overarching goal is to "assure [the] preservation of that degree

[5] In this case, the judge did not find explicitly that the defendant had manifested a subjective expectation of privacy. We infer from the undisputed record, however, that the defendant manifested a subjective expectation of privacy in his location by choosing to meet his codefendant in a quiet residential area. See Commonwealth v. Fulgiam, 477 Mass. 20, 33, cert. denied, 138 S. Ct. 330 (2017) (concluding that subjective prong was satisfied based on record). See, e.g., United States v. Moore-Bush, 381 F. Supp. 3d 139, 143 (D. Mass. 2019) ("the Court infers from their choice of neighborhood that they subjectively expected that their and their houseguests' comings and goings over the course of eight months would not be surreptitiously surveilled").

of privacy against government that existed when the Fourth Amendment [and art. 14 were] adopted." Almonor, 482 Mass. at 54 (Lenk, J., concurring), quoting Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018). We have recognized the difficulty of this enterprise as developing technology places "extraordinarily powerful surveillance tool[s]" in the hands of police. Almonor, supra at 46. See Johnson, 481 Mass. at 716. While acknowledging the usefulness of these tools for crime detection, "both this court and the United States Supreme Court have been careful to guard against the 'power of technology to shrink the realm of guaranteed privacy' by emphasizing that privacy rights 'cannot be left at the mercy of advancing technology but rather must be preserved and protected as new technologies are adopted and applied by law enforcement.'" Almonor, supra at 41, quoting Johnson, supra. See Kyllo v. United States, 533 U.S. 27, 34 (2001). See also Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting) (noting that courts must be vigilant to guard against "[s]ubtler and more far-reaching means of invading privacy [that] have become available to the government").

Like the Supreme Court, this court is guided "by historical understandings of what was deemed an unreasonable search and seizure when [the Constitutions were] adopted." See Almonor, 482 Mass. at 43, citing Carpenter, 138 S. Ct. at 2214. These

historical understandings include the basic purposes underlying the adoption of art. 14 and, later, the Fourth Amendment. See Almonor, supra, quoting Jenkins v. Chief Justice of the Dist. Court Dep't, 416 Mass. 221, 229 (1993) ("we construe [art. 14] in light of the circumstances under which it was framed, the causes leading to its adoption, the imperfections hoped to be remedied, and the ends designed to be accomplished"). See also Carpenter, supra at 2213. More specifically, we have recognized that the underlying purposes of both art. 14 and the Fourth Amendment are the need to "secure the privacies of life against arbitrary power," and to "place obstacles in the way of a too permeating police surveillance." Almonor, supra at 53 (Lenk, J., concurring), quoting Carpenter, supra at 2214. Both warrant further explanation in the context of emerging technology.

A. Arbitrary power. The framers had first-hand experience with abuses of arbitrary power under British rule. Our cases acknowledge that they wrote constitutional search protections 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." See Carpenter, 138 S. Ct. at 2213, quoting Riley v. California, 573 U.S. 373, 403 (2014). See also Commonwealth v. Blood, 400 Mass. 61, 71 (1987). 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. See, e.g., Almonor, 482 Mass. at 46 (police causing cellular telephone to reveal real-time location contravenes reasonable expectation of privacy); Commonwealth v. Augustine, 467 Mass. 230, 255 (2014), S.C., 470 Mass. 837 (2015) (reasonable expectation of privacy exists in cellular site location information [CSLI][6]). See also Carpenter, supra at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere").

B. Permeating police presence. As the Supreme Court made clear in Carpenter, courts analyzing the constitutional implications of new surveillance technologies also should be guided by the founders' intention "to place obstacles in the way of a too permeating police surveillance." Carpenter, 138 S. Ct. at 2214, quoting United States v. Di Re, 332 U.S. 581, 595

[6] Cellular site location information "refers to a cellular telephone service record or records that contain information identifying the base station towers and sectors that receive transmissions from a [cellular] telephone" (citation omitted). Commonwealth v. Estabrook, 472 Mass. 852, 853 n.2 (2015).

(1948). Specifically, both this court and the Supreme Court have recognized how 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.

As Justice Alito wrote in Jones, "[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." United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring). The continuous, tireless, effortless, and absolute surveillance of the digital age contravenes expectations of privacy that are rooted in these historical and practical limitations. For this reason, when the duration of digital surveillance drastically exceeds what would have been possible with traditional law enforcement methods, that surveillance constitutes a search under art. 14. See, e.g., Augustine, 467 Mass. at 253.

In addition, the surreptitious nature of digital surveillance removes a natural obstacle to too permeating a police presence by hiding the extent of that surveillance. Resource constraints aside, 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. Justice Sotomayor summed up these first two concerns in a discussion of global positioning system (GPS)[7] monitoring: "because [it] is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility'" (citation omitted). Jones, 565 U.S. at 415–416 (Sotomayor, J., concurring).

Finally, new surveillance techniques risk creating too permeating a police presence by giving police access to "a category of information otherwise unknowable." Carpenter, 138 S. Ct. at 2218. For example, with CSLI data "the Government can now travel back in time to retrace a person's whereabouts . . . [and] police need not even know in advance whether they want to follow a particular individual, or when. Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years . . . ." Id. See Augustine, 467 Mass.

[7] A global positioning system (GPS) tracking system "allows police to monitor and record the location of a vehicle [or an individual] without the [target]'s knowledge" by ascertaining the target's location via communication with satellites, and then transmitting that location to a computer system that stores it electronically. Commonwealth v. Connolly, 454 Mass. 808, 812 (2009).

at 254. Likewise, in Almonor, 482 Mass. at 46, this court considered the capability of police to "ping" a cellular telephone, causing it to reveal its real-time location data, and observed that "[t]his extraordinarily powerful surveillance tool finds no analog in the traditional surveillance methods of law enforcement."

These historical understandings inform our analysis as we apply the test that originated more than fifty years ago in Katz, 389 U.S. at 361 (Harlan, J., concurring), to determine whether the collection and use of ALPR data constitutes a search.

ii. Searches in public. This founding-era guidance has aided courts, even as technological advances in the surveillance of public space have posed difficult questions to courts under the "reasonable expectation of privacy" framework established in Katz. The tension derives from two contrasting sentences contained in Katz itself. First, Katz states that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Katz, 389 U.S. at 351. For this reason, "[w]hether an expectation of privacy is reasonable depends in large part upon whether that expectation relates to information that has been exposed to the public" (alteration, quotation, and citation omitted). United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010), aff'd in

part sub nom. Jones, 565 U.S. 400. On the other hand, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." Carpenter, 138 S. Ct. at 2217. For "what [someone] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Katz, supra. See id. at 354 (constitutionally protected privacy interest in contents of telephone conversation made from public telephone booth). In short, while the Fourth Amendment and art. 14 "protect[] people, not places," whether something is knowingly exposed to the public remains a touchstone in determining the reasonableness of a person's expectation of privacy. Id. at 351. See Augustine, 467 Mass. at 252; Commonwealth v. Billings, 42 Mass. App. Ct. 261, 265 (1997) (listing constitutional nonsearches based on knowing exposure principle).

A. What is knowingly exposed. Under this doctrine, police observation of the exterior of an automobile is not a search because it is "knowingly exposed." See New York v. Class, 475 U.S. 106, 114 (1986) ("The exterior of a car, of course, is thrust into the public eye, and thus to examine it does not constitute a 'search'"). In Massachusetts, this reasoning extends quite naturally to license plates. In Commonwealth v. Starr, 55 Mass. App. Ct. 590, 591 (2001), a police officer saw a license plate on an automobile, located the plate number in a

police database, and stopped the vehicle because the plates were registered to a different vehicle. Relying on the knowing exposure principle of Katz, the court held that the defendant had no reasonable expectation of privacy that would prevent an officer from examining his license plate. Starr, supra at 593-594.[8]

In United States v. Knotts, 460 U.S. 276, 285 (1983), the Supreme Court applied the logic of "what is knowingly exposed" to sanction the warrantless use of a radio "beeper"[9] to assist police in tracking a vehicle on a single journey.

> "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the codefendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property."

Id. at 281–282. In so holding, the Knotts Court dismissed the defendant's claim that, should he lose his case, "twenty-four

---

[8] Massachusetts requires that license plates be "displayed conspicuously," G. L. c. 90, § 6, and the failure to do so can result in fines or imprisonment, see G. L. c. 90, § 23. These requirements support the contention that there is no objectively reasonable expectation of privacy in a license plate number, the very purpose of which is to identify the vehicle to the government.

[9] "A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver." United States v. Knotts, 460 U.S. 276, 277 (1983).

hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision." Id. at 283. The court went on to note, however, that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." Id. at 284.

In this distinction, we recognize precisely the question posed by this case: whether Knotts, Starr, and the "knowing exposure" principle of Katz control, as the Commonwealth contends, or whether different constitutional principles apply, as the defendant argues. To answer, we must look to those cases of emerging surveillance technology where we indeed have determined that different constitutional principles govern.

B. Mosaic theory. When new technologies drastically expand police surveillance of public space, both the United States Supreme Court and this court have recognized a privacy interest in the whole of one's public movements. See Carpenter, 138 S. Ct. at 2217 ("individuals have a reasonable expectation of privacy in the whole of their physical movements"); Johnson, 481 Mass. at 716; Augustine, 467 Mass. at 248-249; Commonwealth v. Rousseau, 465 Mass. 372, 382 (2013).

The question first emerged in the context of a GPS device affixed to a suspect's vehicle. We ultimately concluded,

consistent with Supreme Court precedent, that "the government's contemporaneous electronic monitoring of one's comings and goings in public places invades one's reasonable expectation of privacy." Rousseau, 465 Mass. at 382. Next, in cases addressing police access to CSLI, both this court and the Supreme Court reaffirmed the same principle -- that it is objectively reasonable for individuals to expect to be free from sustained electronic monitoring of their public movements. See Augustine, 467 Mass. at 247-248. See also Carpenter, 138 S. Ct. at 2219.

Both courts reached these conclusions, in part, by distinguishing the relatively primitive beeper used in Knotts from the encyclopedic, effortless collection of CSLI and GPS data. See Augustine, 467 Mass. at 252 ("There is no real question that the government, without securing a warrant, may use electronic devices to monitor an individual's movements in public to the extent that the same result could be achieved through visual surveillance" [emphasis added]). See also Carpenter, 138 S. Ct. at 2215, 2218 (distinguishing "rudimentary" beeper used in Knotts to track single "discrete automotive journey" from use of CSLI, which achieves "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user").

Essentially, these cases articulate an aggregation principle for the technological surveillance of public conduct, sometimes referred to as the mosaic theory.[10] When collected for a long enough period, "the cumulative nature of the information collected implicates a privacy interest on the part of the individual who is the target of the tracking." Augustine, 467 Mass. at 253. See Jones, 565 U.S. at 416 (Sotomayor, J., concurring) ("when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements . . . I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on" [emphasis added]). A recent case in the United States District Court for the District of Massachusetts summarized the idea succinctly: "Although these activities, taken one by one, may not give rise to a reasonable expectation of privacy . . . , the

[10] See, e.g., Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 (2012) ("The mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps. Instead of asking if a particular act is a search, the mosaic theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group. The mosaic theory is therefore premised on aggregation: it considers whether a set of nonsearches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic").

Court aggregates their sum total for its analysis." United States v. Moore-Bush, 381 F. Supp. 3d 139, 149 (D. Mass. 2019). As the analogy goes, the color of a single stone depicts little, but by stepping back one can see a complete mosaic.

This aggregation principle or mosaic theory is wholly consistent with the statement in Katz, 389 U.S. at 351, that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection," because the whole of one's movements, even if they are all individually public, are not knowingly exposed in the aggregate. As the United States Court of Appeals for the District of Columbia Circuit explained:

> "the whole of a person's movements over the course of a month is not actually exposed to the public because 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."

Maynard, 615 F.3d at 560.

A detailed account of a person's movements, drawn from electronic surveillance, encroaches upon a person's reasonable expectation of privacy because the whole reveals far more than the sum of the parts. "The difference is not one of degree but of kind . . . ." Id. at 562. "Prolonged surveillance reveals types of information not revealed by short-term surveillance,

such as what a person does repeatedly, what he does not do, and what he does ensemble." Id. Aggregated location data reveals "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 of the pattern of our professional and avocational pursuits." Commonwealth v. Connolly, 454 Mass. 808, 834 (2009) (Gants, J., concurring), quoting People v. Weaver, 12 N.Y.3d 433, 442 (2009).

iii. Constitutional implications of ALPRs. With this theoretical foundation in mind, we turn to the central question of this case: whether the use of ALPRs by the police invades an objective, reasonable expectation of privacy. Or, more specifically, we must determine whether ALPRs produce a detailed enough picture of an individual's movements so as to infringe upon a reasonable expectation that the Commonwealth will not electronically monitor that person's comings and goings in public over a sustained period of time. See, e.g., Augustine, 467 Mass. at 247-248.

A. ALPRs under the mosaic theory. In determining whether a reasonable expectation of privacy has been invaded, it is not the amount of data that the Commonwealth seeks to admit in evidence that counts, but, rather, the amount of data that the government collects or to which it gains access. See Commonwealth v. Estabrook, 472 Mass. 852, 858-859 (2015), citing

Augustine, 467 Mass. at 254 ("in terms of reasonable expectation of privacy, the salient consideration is the length of time for which a person's CSLI is requested, not the time covered by the person's CSLI that the Commonwealth ultimately seeks to use as evidence at trial"). In Rousseau, 465 Mass. at 376, 382, we weighed the thirty-one days of GPS monitoring in the constitutional analysis, not the data that placed the vehicle near the suspected arsons on four specific dates. Similarly, in Carpenter, 138 S. Ct. at 2212-2213, the relevant period was the 127 days of CSLI data, not the data that placed the defendant near the robberies on four particular days.[11] For this reason, our constitutional analysis ideally would consider every ALPR

[11] Our holding in Commonwealth v. Johnson, 481 Mass. 710, 722, cert. denied, 140 S. Ct. 247 (2019), is not to the contrary. There, we determined that the imposition of GPS monitoring on a specific probationer was a search, but a reasonable one in the circumstances. Id. at 720. We then concluded that the subsequent examination of the probationer's location data by law enforcement was not a search, because the probationer had no reasonable expectation of privacy in his location; he knew he was wearing a GPS ankle monitor that was transmitting his location to the government. See id. at 722-725, 728. As an ancillary rationale, we emphasized that the police only sought the defendant's location at the specific times of various robberies, thus minimizing the intrusion. Id. at 727-728. Throughout, we emphasized the importance of the individual's status as a probationer, contrasting his expectations of privacy with those of a nonprobationer. Id. at 724 ("There is no question that the reasonableness of any expectations of privacy held by a probationer knowingly subject to GPS monitoring as a condition of probation is far different from the reasonableness of the expectations of privacy held by individuals who are surreptitiously tracked by law enforcement").

record of a defendant's vehicle that had been stored and collected by the government up to the time of the defendant's arrest. That information, however, is not in the record before us.

With enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes. The one-year retention period indicated in the EOPSS retention policy certainly is long enough to warrant constitutional protection. See Augustine, 467 Mass. at 254–255 ("tracking of the defendant's movements [by CSLI] in the urban Boston area for two weeks was more than sufficient to intrude upon the defendant's expectation of privacy safeguarded by art. 14"); Rousseau, 465 Mass. at 382 (thirty-one days of GPS monitoring was sufficient duration to conclude monitoring was search). Like CSLI data, ALPRs allow the police to reconstruct people's past movements without knowing in advance who police are looking for, thus granting police access to "a category of information otherwise [and previously] unknowable." See Carpenter, 138 S. Ct. at 2218. Like both CSLI and GPS data, ALPRs circumvent traditional constraints on police surveillance power by being cheap (relative to human surveillance) and surreptitious.

Of course, the constitutional question is not merely an exercise in counting cameras; the analysis should focus, ultimately, on the extent to which a substantial picture of the defendant's public movements are revealed by the surveillance. For that purpose, where the ALPRs are placed matters too. ALPRs near constitutionally sensitive locations -- the home, a place of worship, etc. -- reveal more of an individual's life and associations than does an ALPR trained on an interstate highway. A network of ALPRs that surveils every residential side street paints a much more nuanced and invasive picture of a driver's life and public movements than one limited to major highways that open into innumerable possible destinations. For while no ALPR network is likely to be as detailed in its surveillance as GPS or CSLI data, one well may be able to make many of the same inferences from ALPR data that implicate expressive and associative rights.[12] See American Civ. Liberties Union Found. of S. Cal. v. Superior Court of Los Angeles County, 3 Cal. 5th

[12] The International Association of Chiefs of Police has warned that collecting ALPR data from multiple sources creates the risk "that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance." International Association of Chiefs of Police, Privacy Impact Assessment Report for the Utilization of License Plate Readers, at 13 (Sept. 2009), https://www.theiacp.org/sites/default/files/all/k-m/LPR_Privacy_Impact_Assessment.pdf [https://perma.cc/M2T4-G5F5].

1032, 1044 (2017) (ALPR data "could potentially reveal where [a] person lives, works, or frequently visits").

Similarly, with cameras in enough locations, the hot list feature could implicate constitutional search protections by invading a reasonable expectation of privacy in one's real-time location. If deployed widely enough, ALPRs could tell police someone's precise, real-time location virtually any time the person decided to drive, thus making ALPRs the vehicular equivalent of a cellular telephone "ping." See Almonor, 482 Mass. at 55 (Lenk, J., concurring) ("When police act on real-time information by arriving at a person's location, they signal to both the individual and his or her associates that the person is being watched. . . . To know that the government can find you, anywhere, at any time is -- in a word -- 'creepy'"). Of course, no matter how widely ALPRs are deployed, the exigency exception to the warrant requirement would apply to this hot list feature.[13]

[13] Order TRF-11 gives a nonexclusive list of reasons for which authorized users may manually place a license plate on a hot list, including "AMBER" alerts, missing child alerts, missing college student bulletins, and "be on the look out" alerts. In these circumstances, the use of real-time alerts may be constitutionally permissible under the exigent circumstances exception to the warrant requirement. See Riley v. California, 573 U.S. 373, 388, 391, 402 (2014) (repeatedly noting how exigent circumstances exception might apply to warrant requirement for cellular telephone searches); Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298–299 (1967) ("The Fourth Amendment does not require police officers to delay in

Finally, like carrying a cellular telephone, driving is an indispensable part of modern life, one we cannot and do not expect residents to forgo in order to avoid government surveillance.

B. Number and location of ALPR data collection points in this case. On this record, however, we need not, and indeed cannot, determine how pervasive a system of ALPRs would have to be to invade a reasonable expectation of privacy. While a testifying expert alluded to cameras "all over the [S]tate," the record is silent as to how many of these cameras currently exist,[14] where they are located, and how many of them detected the defendant.

Therefore, for this case, we consider the constitutional import of four cameras placed at two fixed locations on the ends of the Bourne and Sagamore bridges. "Fourth Amendment [and art. 14] cases must be decided on the facts of each case, not by extravagant generalizations. '[W]e have never held that

---

the course of an investigation if to do so would gravely endanger their lives or the lives of others"). Similarly, the use of ALPRs to find a vehicle reported stolen would not be constitutionally impermissible, because the driver of a stolen vehicle does not have a reasonable expectation of privacy in the location of someone else's automobile.

[14] The amici submit that, in 2015, there were 168 ALPR cameras in operation in Massachusetts. The information provided by the amici was not before the motion judge and remains untested by the adversarial process.

potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment.'" Dow Chem. Co. v. United States, 476 U.S. 227, 238 n.5 (1986), quoting United States v. Karo, 468 U.S. 705, 712 (1984).

"There is no real question that the government, without securing a warrant, may use electronic devices to monitor an individual's movements in public to the extent that the same result could be achieved through visual surveillance." Augustine, 467 Mass. at 252. It is an entirely ordinary experience to drive past a police officer in a cruiser observing traffic on the side of the road, and, of course, an officer may read or write down a publicly displayed license plate number. See Starr, 55 Mass. App. Ct. at 594. In this way, a single license plate reader is similar to traditional surveillance techniques. On the other hand, four factors distinguish ALPRs from an officer parked on the side of the road: (1) the policy of retaining the information for, at a minimum, one year; (2) the ability to record the license plate number of nearly every passing vehicle; (3) the continuous, twenty-four hour nature of the surveillance; and (4) the fact that the recorded license plate number is linked to the location of the observation. These are enhancements of what reasonably might be expected from the police.

The limited number of cameras and their specific placements, however, also are relevant in determining whether they reveal a mosaic of location information that is sufficiently detailed to invade a reasonable expectation of privacy. The cameras in question here gave police only the ability to determine whether the defendant was passing onto or off of the Cape at a particular moment, and when he had done so previously. This limited surveillance does not allow the Commonwealth to monitor the whole of the defendant's public movements, or even his progress on a single journey. These particular cameras make this case perhaps more analogous to CSLI, if there were only two cellular telephone towers collecting data. Such a limited picture does not divulge "the whole of [the defendant's] physical movements," Carpenter, 138 S. Ct. at 2217, or track enough of his comings and goings so as to reveal "the privacies of life." Id., quoting Riley, 573 U.S. at 403. See Boyd v. United States, 116 U.S. 616, 630 (1886).

While we cannot say precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections, it is not that produced by four cameras at fixed locations on the ends of two bridges.[15] Therefore, we conclude

[15] In declining to establish a bright-line rule for when the use of ALPRs constitutes a search, we recognize this may bring some interim confusion. We trust, however, that as our cases develop, this constitutional line gradually and appropriately

that the limited use of ALPRs in this case does not constitute a search within the meaning of either art. 14 or the Fourth Amendment.[16]

b. Defendant's other arguments. We turn to the defendant's remaining claims. He argues that various evidence should be suppressed because (1) the Barnstable police did not show a written policy governing ALPR use, and the State police ALPR policy, adopted by the Barnstable police, is deficient and constitutionally inadequate; (2) the use of ALPR systems violates 18 U.S.C. §§ 2701-2712, the Federal Stored Communications Act (SCA), and 18 U.S.C. §§ 2510-2523, the Federal Electronic Communications Privacy Act (ECPA); (3) the court should adopt the doctrine of target standing; and (4) the incriminating statements were involuntarily coerced through

---

will come into focus. "The judiciary risks error by elaborating too fully on the Fourth Amendment [or art. 14] implications of emerging technology before its role in society has become clear." Ontario v. Quon, 560 U.S. 746, 759 (2010).

[16] The defendant argues that, if the ALPR data were suppressed, there would have been no probable cause for his arrest. Because we conclude that the use of the ALPR data was not a search in the constitutional sense, the data gleaned from the use of the ALPR properly is considered in the probable cause analysis. We discern no error in the motion judge's determination that there was probable cause to arrest the defendant when the ALPR data is included in that analysis.

police trickery in violation of the defendant's Miranda rights.[17] We conclude that each of these arguments is without merit.

i. Role of police policies. The defendant argues that, because the Barnstable police did not introduce a written policy governing police use of ALPR data, and because the State police policy, Order TRF-11, is inadequately specific, the evidence against him must be suppressed. In support of this argument, the defendant relies on cases where we have required police to introduce evidence of a written policy to justify warrantless inventory searches or to demonstrate "that sobriety checkpoints be governed by standard, neutral guidelines that clearly forbid the arbitrary selection of vehicles to be initially stopped." Commonwealth v. Murphy, 454 Mass. 318, 323 (2009) (sobriety checkpoint guidelines). See Commonwealth v. Bishop, 402 Mass. 449, 451 (1988) ("art. 14 . . . requires the exclusion of evidence seized during an inventory search not conducted pursuant to standard police procedures, which procedures, from now on, must be in writing").

[17] In addition to the arguments discussed here, the defendant contends that the seizure of his bail money was unlawful. The seizure of the defendant's bail money was not part of the judge's decision on the motion to suppress and therefore is not properly before this court. See Mass. R. Crim. P. 15 (a) (2), as appearing in 474 Mass. 1501 (2016). Accordingly, we do not consider it.

This argument is unavailing. These cases involve the reasonableness of a search or seizure conducted under specific exceptions to the warrant requirement, not the threshold constitutional question whether a search or seizure has occurred at all. Detailed policy guidelines for police use of ALPRs well may be a "good idea," Riley, 573 U.S. at 398, but their existence or lack thereof does not determine the constitutional question.

ii. Statutory claims. The defendant argues further that the government's use of ALPR data is subject to the SCA and the ECPA. Neither statute, however, is applicable.[18] The SCA prevents the government from compelling a "provider of electronic communication service" to produce such communications without following certain procedures. See 18 U.S.C. § 2703. Here, the government did not compel production of electronic communications, but, rather, created and used them in the first instance. Similarly, the ECPA regulates the interception of

[18] The defendant's reliance on G. L. c. 214, § 1B, is similarly misplaced. That statute creates a cause of action for tort liability to "protect[] individuals from 'disclosure of facts . . . that are of a highly personal or intimate nature when there exists no legitimate, countervailing interest.'" Doe v. Brandeis Univ., 177 F. Supp. 3d 561, 616 (D. Mass. 2016), quoting Dasey v. Anderson, 304 F.3d 148, 153–154 (1st Cir. 2002). While it conceivably could support tort litigation against government actors (subject, of course, to sovereign immunity constraints), it has no application to the criminal suppression context.

wire, oral, and electronic communications. See 18 U.S.C. § 2511. As the motion judge correctly determined, it would produce an absurd reading of the statute to conclude that officers were intercepting their own communications when receiving real-time alerts. See 18 U.S.C. § 2511(2)(c) ("It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication . . ."). See also 18 U.S.C. § 2510(5)(a) (exempting any telephone or equipment used by law enforcement officers in course of their duties from types of devices that can be used to "intercept").

iii. Target standing. The defendant also argues that this court should adopt the doctrine of "target standing," which would give him standing to contest the search of his codefendant because he was one of that search's secondary targets. See Commonwealth v. Santiago, 470 Mass. 574, 577 (2015). It would allow him "to assert that a violation of the Fourth Amendment rights of a third party entitled him to have evidence suppressed at his trial." Id. The United States Supreme Court has rejected the doctrine with respect to the Fourth Amendment. Rakas v. Illinois, 439 U.S. 128, 132-133 (1978). We also repeatedly have declined to adopt target standing under art. 14, but have left open the possibility of applying the doctrine in

cases of "distinctly egregious police conduct." See Santiago, supra at 577-578. Nothing in this record suggests "distinctly egregious police conduct." Therefore, the defendant does not have target standing to challenge evidence seized from his codefendant.

iv. Miranda waiver. The defendant argues that his waiver of his Miranda rights and the statements he made to police were involuntary because the officers repeatedly told him that he was not under arrest. The tests to determine whether a Miranda waiver was voluntary and for the voluntariness of a statement are "essentially the same" (citation omitted). Commonwealth v. Newson, 471 Mass. 222, 229 (2015).

With respect to the Miranda issue, the motion judge found the following. First, the defendant was under arrest at the time he was handcuffed during the roadside stop. He properly and carefully was advised of his Miranda rights immediately after being handcuffed, and again at the police station. He understood these rights both times.

We agree with the motion judge that questions asked at the roadside and at the police station constituted custodial interrogation. Considering the totality of the circumstances, the only factor indicating a lack of voluntariness was the officers' statements that the defendant was not under arrest and that he might avoid arrest by giving the information he

initially promised. The defendant argues that the waiver and the statements were involuntary based on these deceptive representations.

"[D]eception or trickery does not necessarily compel suppression of the confession or admission but, instead, is one factor to be considered in a totality of the circumstances analysis." Newson, 471 Mass. at 230, quoting Commonwealth v. Tremblay, 460 Mass. 199, 208 (2011). In Newson, supra, this court held that even if an officer engaged in deceit or trickery by telling a defendant that he was not under arrest, such deceit would not be enough to demonstrate involuntariness. Here, the facts are essentially the same. Therefore, we do not disturb the judge's finding that the Commonwealth proved beyond a reasonable doubt that the statements and the Miranda waiver were voluntary.

3. Conclusion. While we recognize that the widespread use of ALPRs in the Commonwealth could implicate constitutional protections against unreasonable searches, the limited use of the technology in this case does not.

Order denying motions to suppress affirmed.

GANTS, C.J. (concurring). I agree with the court that, if the State police had obtained historical locational data regarding the defendant's vehicle from enough automatic license plate readers (ALRPs) in enough locations, the mosaic that such collection would create of the defendant's movements "would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes." Ante at . I also agree with the court that the locational information regarding the defendant that was obtained from four ALPRs at two fixed locations on two bridges falls short of creating the type of mosaic that would constitute a search within the meaning of either art. 14 of the Massachusetts Declaration of Rights or the Fourth Amendment to the United States Constitution. And I agree that the court is correct to forbear from declaring in this case "precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections." Id. at . I write separately not to attempt to answer how detailed the picture must be but to suggest an analytical framework that might prove useful in future cases.

It is important to recognize that this is the first case we have encountered where the State police are collecting and storing a vast amount of locational data, from which they potentially might conduct a targeted search of locational information for a particular person or vehicle without probable

cause and without court authorization. Cellular telephone companies possess even more locational data that can track the movements of a cellular telephone (and thus the person in possession of it), but law enforcement may obtain that information from these companies only through a search warrant or court order.

Under our case law, a search warrant based on probable cause is required for law enforcement to obtain more than six hours of historical telephone call cellular site location information (CSLI) regarding a particular individual. See Commonwealth v. Estabrook, 472 Mass. 852, 854 (2015); Commonwealth v. Augustine, 467 Mass. 230, 255 (2014), S.C., 470 Mass. 837 (2015). A court order under 18 U.S.C. § 2703 based on "specific and articulable facts" that show "reasonable grounds to believe" that the records "are relevant and material to an ongoing criminal investigation" suffices under art. 14 to obtain six hours or less of CSLI regarding a particular individual. See Estabrook, supra at 855 n.4, 858. If a law enforcement agency possessed comparable historical locational data that could produce a mosaic of an individual's movements equivalent to that produced by CSLI, whether because it purchased bulk CSLI data from a vendor or because it had a vast array of ALPRs or surveillance cameras using facial recognition software, we would require law enforcement to obtain a search warrant based on

probable cause before it could retrieve the locational data for that mosaic regarding a targeted individual.

But what if the historical locational information regarding a targeted individual that can be obtained from data in the possession of a law enforcement agency could yield a mosaic of location points that is less than that created by CSLI but greater than the four location points established in this record? Pragmatically, I submit we have two alternatives. Our first option is to determine based on the facts of a particular case when the locational mosaic of a targeted individual's movements crosses the threshold of the reasonable expectation of privacy. A mosaic above that threshold would require a search warrant based on probable cause, but a mosaic below that threshold would not require any court authorization.

Alternatively, we could strike a balance analogous to that struck by the United States Supreme Court in Terry v. Ohio, 392 U.S. 1, 21 (1968), and decide that there are two locational mosaic thresholds: a lesser threshold that may be permissibly crossed with a court order supported by an affidavit showing reasonable suspicion and a greater threshold that is permissibly crossed only with a search warrant supported by probable cause. The reasonable suspicion standard would require "specific and articulable facts" demonstrating reasonable suspicion that the targeted individual has committed, is committing, or will commit

a crime, see id. at 21-22, and that there are reasonable grounds to believe that the data obtained from the query are relevant and material to an investigation of the crime. The reasonable suspicion standard is different from and more exacting than the standard required under 18 U.S.C. § 2703 to obtain six hours or less of CSLI, which requires only "specific and articulable facts" that show "reasonable grounds to believe" that the records "are relevant and material to an ongoing criminal investigation."

This second alternative would mean that law enforcement agencies would need to obtain court authorization more often before retrieving targeted individual historical locational information in their possession because queries that would not require a showing of probable cause might still require a showing of reasonable suspicion. But the benefit to law enforcement would be that, if the police sought a court order based on reasonable suspicion and a reviewing court determined that the query sought locational data that could yield a mosaic of movement requiring a showing of probable cause, the search would not be found unconstitutional (and the information collected would not be suppressed) if the reviewing court found that the affidavit supported a finding of probable cause. In contrast, where no court order was obtained and a reviewing court determined that probable cause or reasonable suspicion was

required to support the retrieval of historical locational information, the data retrieved from the query would have to be suppressed even if law enforcement could have met the applicable standard.

Regardless of which alternative the court ultimately chooses, a reviewing court will need to know the extent of the mosaic that was possible from the retrieval of historical locational information regarding the movements of a targeted individual, because only then can the court accurately determine whether the threshold had been crossed. Therefore, unless the law enforcement agency has sought prior court approval to search for particularized locational data in its possession, the agency will have to preserve each and every search query for the retrieval of historical locational information regarding a targeted individual. For instance, if the State police maintain 1,000 ALPRs at different locations throughout the Commonwealth, it matters whether they searched for a suspect's vehicle from the data yielded by all 1,000 cameras or only by four cameras, and it matters whether they gathered this data for one day or one hundred days. And regardless of whether a court authorized the search, the agency must preserve the historical locational data regarding a particular individual that the agency retrieved as a result of such queries from the data in its possession, even when that exceeds the amount of data that the agency uses

in an investigation or at trial. Cf. Estabrook, 472 Mass. at 859 ("the salient consideration is the length of time for which a person's CSLI is requested, not the time covered by the person's CSLI that the Commonwealth ultimately seeks to use as evidence at trial"). And the agency must make this preserved data and search request available in discovery when sought by the defendant. Only then will a court have the information it needs to determine whether the retrieval of locational information regarding a targeted individual crossed a constitutional threshold that requires court authorization and either reasonable suspicion or probable cause.