CRIMINAL PROCEDURE — FOURTH AMENDMENT — MASSACHUSETTS SUPREME JUDICIAL COURT HOLDS THAT USE OF AUTOMATED LICENSE PLATE READERS MAY CONSTITUTE A SEARCH. — *Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020).

In 2016 and 2017, U.S. law enforcement scanned 2.5 billion license plates, 99.5% of which belonged to vehicles unassociated with criminal activity.[1] The first appellate court in the country to address whether use of automated license plate readers[2] (ALPRs) constitutes a search under the Fourth Amendment,[3] the Massachusetts Supreme Judicial Court (SJC) in *Commonwealth v. McCarthy*[4] considered the surveillance's duration, surreptitiousness, and categories of information in its analysis.[5] The SJC held that while "widespread use" of ALPRs can constitute a search, the limited use thereof in this case did not.[6] Given the case's limited facts, *McCarthy* just scratched the surface of ALPRs' use in Fourth Amendment search doctrine. This comment identifies practical realities of ALPRs that may merit greater constitutional scrutiny in future cases, owing to the potentially indefinite duration of ALPR data; the opaque, public-private nature of many ALPR databases; and the scale and categories of information revealed by ALPR surveillance.

In early 2017, Barnstable police began to suspect Jason McCarthy of supplying heroin to a co-conspiring distributor in Cape Cod.[7] As part of their investigation, the police added McCarthy's vehicle to an ALPR hot list on February 1, 2017, to observe when and how frequently the vehicle crossed the Bourne or Sagamore bridges onto the Cape.[8] They additionally tracked — both retroactively and prospectively — every time the vehicle crossed the two bridges between December 1, 2016, and

---

[1] *See* Tanvi Misra, *Who's Tracking Your License Plate?*, BLOOMBERG CITY LAB (Dec. 6, 2018, 9:31 AM), https://www.bloomberg.com/news/articles/2018-12-06/why-privacy-advocates-fear-license-plate-readers [https://perma.cc/ZG3W-NJ3H].

[2] "Automatic license plate readers are cameras [that] . . . identify and 'read' license plates on passing vehicles" through sophisticated technology. Commonwealth v. McCarthy, 142 N.E.3d 1090, 1095 (Mass. 2020). ALPRs record photographs of the license plates they identify, along with a vehicle's license plate number, travel lane, date, time, location, and the direction of travel. *Id.*

[3] *See* Orin S. Kerr, *Automated License Plate Readers, the Mosaic Theory, and the Fourth Amendment*, VOLOKH CONSPIRACY (Apr. 22, 2020, 5:46 AM), https://reason.com/volokh/2020/04/22/automated-license-plate-readers-the-mosaic-theory-and-the-fourth-amendment [https://perma.cc/BE6T-CBQB].

[4] 142 N.E.3d 1090.

[5] *Id.* at 1099.

[6] *Id.* at 1095.

[7] *Id.* at 1096.

[8] *Id.* This information feeds into a database maintained, in Massachusetts, by the Executive Office of Public Safety and Security. *Id.* at 1095. The Massachusetts State Police Department owns and maintains the ALPRs. *Id.*

February 12, 2017.[9] On February 8, 2017, Barnstable police received an ALPR alert that McCarthy's vehicle was driven over the Sagamore Bridge onto the Cape; officers then tailed the defendant and the distributor to a meet-up point, where the two met and shortly departed, absent a physical exchange.[10] The police observed a similar interaction on February 22, 2017.[11] Suspecting a heroin transaction, Barnstable police arrested both the distributor — finding heroin on his person — and McCarthy.[12] McCarthy filed motions to suppress, inter alia, the ALPR data, which a Superior Court judge denied.[13] He then pursued an interlocutory appeal in the SJC, arguing that the police's use of ALPRs constituted a search under the Fourth Amendment of the U.S. Constitution[14] or article 14 of the Massachusetts Declaration of Rights.[15]

Writing for the court, Justice Gaziano[16] applied the *Katz v. United States*[17] test,[18] concluding that though the defendant had a reasonable "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."[19] In assessing privacy expectations over time, the "overarching goal" is to preserve "that degree of privacy against government that existed when the Fourth Amendment [and article 14 were] adopted."[20] "[T]he underlying purposes" are "to 'secure the privacies of life against arbitrary power,' and to [curtail] 'a too permeating police surveillance.'"[21] On arbitrary power, the Framers sought to prevent British officials' "warrantless rummaging" through the home; likewise, police's use of "complex digital trails and location records" should be restricted today.[22] Moreover, the traditional protections against "a too permeating police surveillance"[23] — practical and logistical constraints[24] — are no longer as salient with today's advanced surveillance technologies. With these Founding-era principles in mind, the court

---

[9] *Id.* at 1096.

[10] *Id.*

[11] *Id.* at 1097.

[12] *Id.*

[13] *Id.*

[14] U.S. CONST. amend. IV.

[15] MASS. CONST. pt. 1, art. XIV; *McCarthy*, 142 N.E.3d at 1097.

[16] Justice Gaziano was joined by Chief Justice Gants and Justices Lenk, Lowy, Budd, Cypher, and Kafker.

[17] 389 U.S. 347 (1967).

[18] *Id.* at 361 (Harlan, J., concurring).

[19] *McCarthy*, 142 N.E.3d at 1095 (emphases added).

[20] *Id.* at 1098 (quoting Commonwealth v. Almonor, 120 N.E.3d 1183, 1200 (Mass. 2019) (Lenk, J., concurring)).

[21] *Id.* (quoting *Almonor*, 120 N.E.3d at 1200 (Lenk, J., concurring)).

[22] *Id.* at 1099.

[23] *Id.* (quoting Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018)).

[24] *See id.*

identified three means by which modern surveillance might exceed historical limits. The court analyzed (1) the search's duration, (2) its surreptitious nature, and (3) the access it may grant to otherwise unknowable categories of information,[25] which includes the police's newfound ability both to ascertain real-time location data and to "travel back in time to retrace a person's whereabouts."[26]

The court then analyzed whether ALPRs' use may constitute a Fourth Amendment search under *Katz*, in conversation with *United States v. Jones*[27] and *Carpenter v. United States*.[28] Items "knowingly exposed" to the public, like license plates, are generally unprotected;[29] and those traveling in vehicles "on public thoroughfares" lack protected privacy interests in their "movements from one place to another," that is, "on a single journey."[30] Nonetheless, as *Carpenter* clarified, individuals have protected privacy interests "in the *whole* of their physical movements,"[31] which, though "individually public, are not knowingly exposed in the aggregate."[32] In embracing this aggregation principle,[33] the court explained that twenty-four-hour "dragnet-type" surveillance,[34] if it occurred, may encroach upon protected privacy interests "because the whole reveals far more than the sum of the parts."[35]

If ALPR technology produces a detailed-enough picture to reveal a mosaic of one's daily life, the court reasoned, its use may constitute a search under the Fourth Amendment and article 14.[36] Justice Gaziano thus concluded that "[w]ith enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would

---

[25] *Id.* at 1099–100.

[26] *Id.* at 1100 (quoting *Carpenter*, 138 S. Ct. at 2210).

[27] 565 U.S. 400 (2012) (analyzing GPS use in the Fourth Amendment context).

[28] 138 S. Ct. 2206 (analyzing cell-site location information use); *McCarthy*, 142 N.E.3d at 1100–06.

[29] *McCarthy*, 142 N.E.3d at 1101.

[30] *Id.* (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).

[31] *Carpenter*, 138 S. Ct. at 2217 (emphasis added).

[32] *McCarthy*, 142 N.E.3d at 1103 (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

[33] That is, constitutionally protected privacy interests may be implicated where information obtained is sufficiently cumulative in the aggregate. *Id.* at 1102–03; *see also id.* at 1102 & n.10 (citing Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012)).

[34] *Id.* at 1101 (quoting *Knotts*, 460 U.S. at 284).

[35] *Id.* at 1103. In analyzing whether "sustained electronic monitoring" by advanced technologies reveals too much, courts also consider whether ordinary visual surveillance could achieve the same result. *See id.* at 1102.

[36] *See id.* at 1103. Note that the aggregation principle applies not just to the ALPR-related materials that the government wishes to introduce into evidence, but also to "the amount of data that the government collects or to which it gains access" through ALPRs in the first instance. *Id.*

invade a reasonable expectation of privacy."[37] The surveillance's duration, surreptitiousness, and the categories of information it unveils to law enforcement all weigh in the analysis, as do ALPRs' placement.[38]

In this case, however, only four cameras were deployed, at two fixed locations, on two discrete bridges, to surveil McCarthy's movements over a two-and-a-half-month period.[39] While the court declined to define the line at which ALPRs' use "invoke[s] constitutional protections," Justice Gaziano wrote, "it is not [this]."[40] The surveillance was sufficiently limited to prevent the government from "monitor[ing] the whole of [McCarthy's] public movements," providing merely "a limited picture" thereof.[41] The court held that while more extensive usage of ALPR technology might constitute a search, in this case the limited use thereof did not, affirming the order below.[42]

Chief Justice Gants concurred, agreeing that if the data had been obtained "from enough [ALPRs] in enough locations," the resulting mosaic might have constituted a search; and he declined to promulgate a bright-line rule as to when that threshold might be passed.[43] He instead proposed a *Terry*-like[44] analytical framework for ALPR cases, with "two locational mosaic thresholds."[45] The first was a "lesser threshold" for ALPR uses revealing a lesser picture of one's movements; it "may be permissibly crossed with a court order supported by an affidavit showing reasonable suspicion" (similar to a *Terry* stop).[46] The second was "a greater threshold [requiring] a search warrant [and] probable cause."[47] He argued that this framework would benefit law enforcement and reviewing courts, which could determine whether the query revealed too much in the aggregate and, further, whether the affidavit could have supported probable cause — rendering the evidence admissible.[48]

In reviewing this case of first impression, the *McCarthy* court began the doctrinal conversation about whether use of ALPRs may constitute a search under the *Katz* privacy test, as informed by *Jones* and *Carpenter*. The court identified three relevant factors: duration, surreptitiousness, and access to new categories of information.[49] A closer look

---

[37] *Id.* at 1104.

[38] *See id.* That is, placement "near constitutionally sensitive locations," such as residences or places of worship, may impermissibly "implicate expressive and associative rights." *Id.*

[39] *Id.* at 1106.

[40] *Id.*

[41] *See id.*

[42] *Id.* at 1106, 1109. The court disposed of McCarthy's remaining claims. *See id.* at 1106–08.

[43] *Id.* at 1109 (Gants, C.J., concurring).

[44] *See* Terry v. Ohio, 392 U.S. 1, 21 (1968).

[45] *See McCarthy*, 142 N.E.3d at 1110 (Gants, C.J., concurring).

[46] *Id.*

[47] *Id.*

[48] *See id.*

[49] *Id.* at 1098–99 (majority opinion).

at the technology's practical realities, however, reveals that ALPRs present unique privacy concerns, beyond those analyzed in *Jones* and *Carpenter* in the GPS and cell-site location information (CSLI) contexts. In future cases, ALPR use may merit greater constitutional scrutiny, given the technology's potentially indefinite duration; surreptitious, public-private nature; and facilitation of access to new categories of information, on an unprecedented scale.

First, ALPRs may threaten reasonable expectations of privacy in their potentially indefinite duration of data collection and retention. GPS and CSLI data are typically obtained by law enforcement post hoc,[50] for relatively limited time periods,[51] and, for CSLI, with a relatively short data retention period.[52] ALPRs can send real-time alerts with contemporaneous location information, collected automatically and recurrently; and they can cover both prospective *and* retrospective periods, spanning back for potentially years, if not decades.[53] The ALPR database in *McCarthy* was owned and operated by Massachusetts state agencies, with a one-year data retention policy for historical data.[54] While the government's own ALPR cameras may include procedural safeguards — including transparency requirements, data retention limitations, and other democratically approved policies — those of the private sector may not.[55] Critically, when private-sector ALPR companies collect and store ALPR data indefinitely, that information may become available to contracting law enforcement agencies that subscribe to these less rights-protective databases.[56] To the extent that courts have ruled it "objectively reasonable . . . to expect to be free from sustained elec-

---

[50] *See* Kerr, *supra* note 33, at 330–33.

[51] *See* United States v. Jones, 565 U.S. 400, 412 (2012) (Alito, J., concurring) (arguing that a four-week investigation was "surely" long enough to constitute a search in the GPS data context); *cf. id.* at 415 (Sotomayor, J., concurring) (agreeing with Justice Alito, and his three cosigning Justices for a total of five, that "longer term GPS [surveillance] impinges on expectations of privacy"). *But see McCarthy*, 142 N.E.3d at 1105–06 (holding a two- to three-month period of ALPR data collection to be permissible, suggesting further apparent durational differences between the technologies).

[52] *See, e.g.*, Rob Pegoraro, *Apple and Google Remind You About Location Privacy, But Don't Forget Your Wireless Carrier*, USA TODAY (Nov. 23, 2019, 6:00 AM), https://www.usatoday.com/story/tech/columnist/2019/11/23/location-data-how-much-do-wireless-carriers-keep/4257759002 [https://perma.cc/9AHR-GZLZ] (noting CSLI data's one- to five-year retention periods).

[53] That is, ALPRs automatically and recurrently record snapshots of every passing license plate; compare CSLI or GPS devices, which tend to track individuals' movements over more discrete periods of time. *See* Stephanie Foster, Note, *Should the Use of Automated License Plate Readers Constitute a Search After* Carpenter v. United States*?*, 97 WASH. U. L. REV. 221, 239 (2019).

[54] *See McCarthy*, 142 N.E.3d at 1096. *But see id.* at n.3 (noting a lack of analogous restrictions for *real-time* alerts — that is, "[emails] sent after a real-time alert may be retained . . . indefinitely").

[55] Dave Maass, *The Four Flavors of Automated License Plate Reader Technology*, ELEC. FRONTIER FOUND. (Apr. 6, 2017), https://www.eff.org/deeplinks/2017/04/four-flavors-automated-license-plate-reader-technology [https://perma.cc/2TTX-S8JM].

[56] *See id.*; *see also LPR Usage and Privacy Policy*, VIGILANT SOLS., https://www.vigilantsolutions.com/lpr-usage-and-privacy-policy [https://perma.cc/7ZXL-BSFZ] (explaining that one company maintains its private ALPR data "as long as it has commercial value").

tronic monitoring" of the whole of one's public movements,[57] law enforcement's access to indefinite (and theoretically infinite), retroactive, contemporaneous, and prospective location data may indeed represent the "dragnet-type" law enforcement that the *McCarthy* court feared.

Second, the surreptitiousness of ALPR technology may likewise extend beyond that identified by the *McCarthy* court,[58] again owing to ALPR databases' mutually constitutive public-private nature. One illustrative example concerns Vaas International Holdings, Inc. (Vaas), a private corporation whose networks aggregate scans from ALPR cameras stationed across the country into extensive ALPR databases.[59] Law enforcement agencies can subscribe to one of Vaas's networks, Vigilant Solutions,[60] which is among the nation's largest ALPR vendors.[61] Vigilant Solutions sells to police departments access to a database containing over five billion ALPR scans collected nationwide, about 1.5 billion of which originate from other law enforcement agencies.[62] This "creates a revolving door of license plate scans from law enforcement to Vigilant Solutions back to law enforcement agencies."[63] Problems of surreptitiousness that arise from this contractual system extend beyond the public's probable lack of knowledge as to its workings or its existence. First, transparency and procedural safeguards (e.g., data retention limitations) may be lacking altogether in private vendors' ALPR databases.[64] Second, vendor contracts with private ALPR companies may prohibit law enforcement from disclosing to the public their use of the ALPR surveillance systems' private databases, even if they wanted to.[65] ALPRs differ in this way from GPS devices, which must be physically placed onto targets' persons, vehicles, or belongings, and CSLI, which generally must be obtained from targets' cell phone companies via warrants.[66] ALPRs, however, can surreptitiously collect and distribute an untold aggregation of individuals' location data — not

---

[57] *See McCarthy*, 142 N.E.3d at 1102 (citing cases in the CSLI context).

[58] *See id.* at 1099–100.

[59] *See* Julia M. Brooks, *Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia*, 25 RICH. J.L. & TECH. 1, 10 (2019).

[60] *See id.*

[61] *Street-Level Surveillance: Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/4SH9-NRP2].

[62] Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations [https://perma.cc/HGE5-9BXF].

[63] *Id.*

[64] *See* Maass, *supra* note 55.

[65] *See, e.g.*, VIGILANT SOLUTIONS, STATE AND LOCAL LAW ENFORCEMENT AGENCY AGREEMENT § 4(d)–(e) (2016), https://assets.documentcloud.org/documents/4618380/ITEM-4-Contract-No-DP8119104I-FY-16-17.pdf [https://perma.cc/CCK5-77XY].

[66] *See, e.g.*, Díaz & Levinson-Waldman, *supra* note 62.

only over a potentially indefinite duration, but also across the country, in ways likely unknown to the general public. Traditional surveillance could not furtively obtain such a wide breadth of information, heightening constitutional privacy concerns further still.

Third, though unapparent from this case, ALPRs differ from their doctrinal predecessors in the scale and categories of information on which they can collect data. CSLI arguably invokes constitutionally protected categories of information insofar as cell phones are typically carried on the target's person, thereby following her in and around traditionally protected spaces, such as the home, places of worship, and other places of association.[67] GPS devices — affixed proximately to individuals' vehicles, persons, or belongings — present analogous concerns.[68] ALPRs, by contrast, may appear less intrusive at first blush: they are often stationary devices located on street poles, traffic lights, freeway exit ramps, and the like — that is, traditionally unprotected[69] public streets.[70] Semistationary ALPR cameras — which law enforcement may place in strategic locations, like monitored parking lots — are likewise essentially immobile during the specified period of surveillance; and mobile ALPR cameras are typically affixed to police patrol cars or surveillance vehicles, not to a target's person.[71] While mobile ALPRs can follow an individual to track her movements, this activity hardly differs from that of ordinary surveillance (no new categories of information here).[72] In this sense, ALPRs may be unlikely to gather an unusually broad scale of information on one's movements in the way that CSLI and other more target-proximate and mobile forms of location-based tracking may do.[73] In this case, four stationary cameras affixed to two bridges on public highway overpasses did not impermissibly invade McCarthy's reasonable privacy expectations.[74] On *McCarthy*'s

---

[67] *See, e.g.*, *McCarthy*, 142 N.E.3d at 1109 (Gants, C.J., concurring); Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[68] *See* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *see also* Commonwealth v. Mora, 150 N.E.3d 297, 303, 308 (Mass. 2020) (holding that targeted camera surveillance of the home presents similar concerns as do GPS and CSLI).

[69] *See* Foster, *supra* note 53, at 222–23.

[70] *See* Maass, *supra* note 55.

[71] *See id.*; *see also* Foster, *supra* note 53, at 221.

[72] Mobile ALPR surveillance differs insofar as Fourth Amendment interests of *nontargeted* individuals are concerned, but less so in terms of recording the license plate of a targeted individual in the police officer's proximity. That is, while a police officer in traditional surveillance may theoretically — but, in practice, likely will not — record the license plates of every single other (nontargeted, and hence possibly lacking in individuated suspicion) vehicle in the area, mobile ALPRs automatically record up to 1,800 license plates per minute, capturing all those in the vicinity without pause, reason, or circumscription. *See* Foster, *supra* note 53, at 226.

[73] *See McCarthy*, 142 N.E.3d at 1102. It is indeed the case that ALPRs may track, as the *McCarthy* court notes, individuals' movements over a more expansive area and duration, incomparable to that capable of being assessed by ordinary surveillance. This point is taken up below.

[74] *See id.* at 1105–06.

facts, ALPR technology may appear less invasive than other forms of tracking, as concerns the scale of the categories-of-information factor.

However, the integration of ALPR data across government agencies and the private sector underscores not only the unprecedented durational categories of information that ALPRs reveal, but also the tools' cross-jurisdictional information-sharing consequences. In *McCarthy*, a state agency managed the ALPR databases for cameras owned and operated by the state police.[75] But a major constitutional implication of the categories-of-information factor arises from the aforementioned practical integration of government agencies' local ALPR systems with those of the national private sector.[76] While one unique category of information exposed by ALPRs concerns law enforcement's newfound ability to "travel back in time," the public-private nature of ALPRs *extends* this duration to a potentially indefinite, nationwide, cross-jurisdictional scale. Recordation and aggregation on such a wide scale may enable the government "to ascertain, more or less at will, [individuals'] political and religious beliefs, sexual habits, and so on" — the exact "dragnet" surveillance feared by the *McCarthy* court.[77] Of constitutional import, the scale of information uncovered by such sweeping surveillance may reveal "a highly detailed profile, not simply of where we go, but . . . of our associations — political, religious, amicable and amorous . . . — [and] the pattern of our professional and avocational pursuits."[78] Further, "the only way to opt out of [ALPR] surveillance is to avoid the impacted area, which may pose significant hardships and be . . . unrealistic."[79] Though this scaling consequence was not implicated by the facts of *McCarthy*, it is nonetheless germane when analyzing ALPRs under the *Katz-Jones-Carpenter* framework going forward.

Overall, in conducting its fact-specific analysis on ALPR use in this case, the *McCarthy* court just scratched the surface of the broader implications of ALPR technology in Fourth Amendment search doctrine. ALPRs' practical realities raise concerns regarding these databases' potentially indefinite duration, lack of transparency in their public-private nature, and facilitation of access to new categories of information on an unprecedented scale. ALPRs' use therefore may merit greater constitutional scrutiny in future Fourth Amendment cases.

---

[75] *Id.* at 1095.

[76] *See, e.g.*, Maass, *supra* note 55.

[77] *McCarthy*, 142 N.E.3d at 1102 (quoting United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring)); *see also* Commonwealth v. Mora, 150 N.E.3d 297, 312 (Mass. 2020) ("The resulting mosaic is 'a category of information [traditionally unavailable].'" (citation omitted)).

[78] *McCarthy*, 142 N.E.3d at 1103 (quoting Commonwealth v. Connolly, 913 N.E.2d. 356, 377 (Mass. 2009) (Gants, J., concurring)).

[79] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE CBP LICENSE PLATE READER TECHNOLOGY 7 (2020); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (explaining that a cell phone is "indispensable to participation in modern society").