COMMONWEALTH OF MASSACHUSETTS

Supreme Judicial Court

No. SJC-12750

COMMONWEALTH,
APPELLEE,

v.

JASON MCCARTHY,
APPELLANT.

ON APPEAL FROM A JUDGMENT OF THE SUPERIOR COURT

BRIEF AMICUS CURIAE
OF THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS, INC., COMMITTEE FOR PUBLIC COUNSEL SERVICES, THE ELECTRONIC FRONTIER FOUNDATION, AND THE MASSACHUSETTS ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

Jessie J. Rossman (BBO 670685)
Matthew R. Segal (BBO 654489)
American Civil Liberties Union Foundation of Massachusetts, Inc.
211 Congress Street
Boston, MA 02110
(617) 482-3170
jrossman@aclum.org

Matthew Spurlock (BBO 601156)
David Rangaviz (BBO 681430)
Committee for Public Counsel Services
Public Defender Division
44 Bromfield Street
Boston, MA 02108
(617) 910-5727
mspurlock@publiccounsel.net

Nathan Freed Wessler (BBO 680281)
Ashley Gorski (*on the brief*)
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

ON THE BRIEF:
Jennifer Lynch (CA 240701)
Andrew Crocker (CA 291596)
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jlynch@eff.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21, the American Civil Liberties Union of Massachusetts, Inc. (ACLUM) and the Electronic Frontier Foundation (EFF) represent that they are 501(c)(3) organizations under the laws of the Commonwealth of Massachusetts. The Massachusetts Association of Criminal Defense Lawyers (MACDL) represents that it is a 501(c)(6) organization under the laws of the Commonwealth of Massachusetts. The American Civil Liberties Union (ACLU) is a District of Columbia non-profit membership organization and 501(c)(4) organization. ACLU, ACLUM, EFF and MACDL do not issue any stock or have any parent corporation, and no publicly held corporation owns stock in ACLU, ACLUM, EFF or MACDL.

PREPARATION OF AMICUS BRIEF

Pursuant to Appellate Rule 17(c)(5), amici and their counsel declare that:

(a) no party or party's counsel authored this brief in whole or in part;

(b) no party or party's counsel contributed money to fund preparing or submitting the brief;

(c) no person or entity other than the amici curiae contributed money that was intended to fund preparing or submitting a brief; and

(d) counsel has not represented any party in this case or in proceedings involving similar issues, or any party in a case or legal transaction at issue in the present appeal.

INTRODUCTION

As with cell phones, cars have long been "such a pervasive and insistent part of daily life" that for many individuals, owning and driving one "is indispensable to participation in modern society." *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (cleaned up).[1] Our vehicles take us to private places like our homes, doctors' offices, and places of worship. And yet, for many years now, with little to no oversight, law enforcement agencies have been using Automated License Plate Readers (ALPRs) to scan and record the locations of billions of vehicles' license plates across the country, logging people's travels and revealing their "privacies of life." *Id*. at 2217.

ALPRs are only able to capture this wealth of information due to technological innovation: their computer-controlled camera systems automatically capture images of every license plate that comes into view. These systems collect and store data on every vehicle they encounter, regardless of whether individual drivers are suspected of criminal activity. This data includes not just the plate number but also a photograph of the vehicle and detailed time, data and location information that can place the vehicle to within feet of the original scan.

As in many cases, police here used ALPRs in two ways.

[1] "This brief uses (cleaned up) to indicate that internal quotation marks, alterations or citations have been omitted from quotations." Jack Metzler, *Use (cleaned up) to make your legal writing easier to read*, (Oct. 3, 2017), Before the Bar, abaforlawstudents.com/2017/10/03/use-cleaned-up-make-legal-writing-easier-to-read/; *see also* Jack Metzler, *Cleaning up quotations*, 18 Journal of Appellate Practice and Process 143 (2017).

First, they obtained at least 128 detailed historical location records reflecting each time the car driven by Mr. McCarthy passed along the Bourne or Sagamore Bridges over a two-month period. Second, they added the car's plate to a "hot list," and received at least a dozen real-time alerts each time this vehicle passed by ALPR cameras on the bridges. Cumulatively, the police obtained at least 155 detailed historical and real-time location records.[2] Because the bridges represent the only motor vehicle routes into and out of Cape Cod, police were able to build a detailed portrait of Mr. McCarthy's travels using just these two fixed surveillance points.

The District Attorney suggests that these actions do not require a warrant because "it is simply unreasonable for any person to believe that their public conduct should remain private from observation in today's society, where there is a significant amount of video surveillance." Comm. Br. at 36. Yet this Orwellian outcome is exactly what art. 14 and the Fourth Amendment are meant to protect against. Both this Court and the United States Supreme Court have taken pains to ensure that technology does not "shrink the realm of guaranteed privacy."

[2] Beyond the 128 historical location records and the 12 real-time location records discussed above, there are an additional 15 location records from February 2 - 12, 2017, which were not included in the produced emails, but were included in the spreadsheet in the Record Appendix ("R.A."). *See* Ex. 2 at 64; Ex. 3. Because it is unclear whether these location records were obtained retrospectively or as real-time alerts, this brief counts them only towards the total number of location records obtained by the police—155—and does not include them in the count of either the historical or real-time location records.

Commonwealth v. Almonor, 482 Mass. 35, 47 (2019) (quoting *Kyllo v. United States,* 533 U.S. 27, 34-35 (2001)). ALPRs give police previously unimaginable capabilities: the ability to effortlessly track an individual for days or weeks on end, to enter a virtual time machine to review past movements, or to instantaneously pluck an individual's real-time location out of thin air. Deployed without a warrant, these novel powers fundamentally undermine the "degree of privacy against government that existed when the Fourth Amendment" and art. 14 were adopted. *Carpenter*, 138 S. Ct. at 2214 (cleaned up). To prevent these capabilities from feeding "a too permeating police surveillance," this Court should hold that ALPRs trigger the warrant requirement where, as here, police use the technology to obtain location information "otherwise unknowable" via traditional surveillance. *Id.* at 2214, 2218 (cleaned up).

STATEMENT OF INTEREST OF AMICI

The American Civil Liberties Union of Massachusetts, Inc. (ACLUM) and the American Civil Liberties Union (ACLU) are membership organizations dedicated to the principles of liberty and equality embodied in the constitutions and laws of the Commonwealth and the United States. The rights they defend through direct representation and amicus briefs include the right to be free from unreasonable searches and seizures. *See, e.g., Commonwealth v. Almonor,* 482 Mass. 35 (2019) (amicus); *Commonwealth v. Augustine*, 467 Mass. 230 (2014)(direct representation); *Carpenter v. United States*, 138 S. Ct. 2206

(2018) (direct representation); *United States v. Jones*, 565 U.S. 400 (2012) (amicus).

The Committee for Public Counsel Services (CPCS), Massachusetts's public defender agency, is statutorily mandated to provide counsel to indigent defendants in criminal proceedings. G.L. c. 211D, § 5. The rights that CPCS defends through direct representation and amicus briefs include the right to be free from unreasonable searches and seizures. *See, e.g., Commonwealth v. Almonor*, 482 Mass. 35 (2019); *Commonwealth v. Johnson*, 481 Mass. 710 (2019). The issue addressed in this case will affect numerous indigent defendants whom CPCS attorneys are appointed to represent.

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for nearly 30 years. EFF represents technology users' interests in court cases and broader policy debates. EFF has served as amicus in numerous cases addressing Fourth Amendment protections for technologies that involve location tracking, including *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018); *Commonwealth v. Augustine*, 467 Mass. 230 (2014); *United States v. Jones*, 565 U.S. 400 (2012).

The Massachusetts Association of Criminal Defense Lawyers (MACDL) is an incorporated association representing more than 1,000 experienced trial and appellate lawyers who are members of the Massachusetts Bar and who devote a substantial part of their practices to criminal defense. MACDL files amicus in cases

raising questions important to the criminal justice system.

STATEMENT OF THE CASE AND FACTS

Amici adopt Mr. McCarthy's statement of the facts and provide the following information concerning ALPR technology.

I. ALPR systems across the country automatically and indiscriminately scan license plate data, including detailed location information.

By design, ALPR collection is indiscriminate. ALPR cameras automatically scan and capture images of every license plate that comes into view, regardless of any association with criminal activity. In a 2018 nationwide survey of 173 law enforcement agencies, EFF and MuckRock discovered that an average of 99.5% of the ALPR scans belonged to cars that were *not* associated with any crime.[3]

ALPR cameras may be mounted on fixed points, squad cars or movable trailers that can be placed temporarily and covertly at locations of interest.[4] ALPRs detect when a license plate enters the camera's field, capture a photograph of the car and its surroundings (including the plate), capture an infrared image of the plate at night, and convert the image of the plate into alphanumeric data—in effect "reading" the plate.[5]

---

[3] Tanvi Misra, *Who's Tracking Your License Plate?*, Citylab (Dec. 6, 2018), https://www.citylab.com/equity/2018/12/automated-license-plate-readers-privacy-data-security-police/576904/.
[4] Northern California Fusion Center Has 3 Covert ALPR Trailers to Loan Out, Ctr. for Human Rights and Privacy, https://www.cehrp.org/northern-california-fusion-center-has-3-covert-alpr-trailers-to-loan-out/.
[5] *See* Allison Klein & Josh White, *License plate readers: A useful tool for police comes with privacy concerns*, Washington Post (Nov. 19, 2011) https://www.washingtonpost.com/local/license-

ALPRs record data on every plate they scan, including the precise time, date, and place it was encountered, uploading this information to a database almost immediately after the scan.[6] ALPR systems record detailed geolocation data for each plate scanned, including, in this case, not just the location of the ALPR camera itself, but the direction and specific lane in which the car was traveling.[7] ALPR systems can even generate precise GPS information, which is accurate enough to record an ALPR's location to a distance of two to four inches and to pinpoint the location of the car whose plate was scanned within several feet.[8]

II. ALPRs collect a significant amount of data.

By scanning every license plate that comes into view—up to 1,800 plates per minute[9]—ALPRs collect an enormous volume of data. For example, the ALPR cameras on the Bourne and Sagamore bridges, which photograph the plate of every vehicle that enters or leaves Cape Cod, have recorded "more than 100 million

---

plate-readers-a-useful-tool-for-police-comes-with-privacy-concerns/2011/11/18/gIQAuEApcN_story.html; Misra, *Who's Tracking Your License Plate?, supra* note 3; Excerpts of Record at 163-165, 175, 206-207, *United States v. Yang*, No. 18-10341 (9th Cir.), Dkt. No. 7 (Testimony of Todd J. Allen Hodnett), (hereinafter "Hodnett Testimony").

[6] *See* Klein & White, *License plate readers: A useful tool for police comes with privacy concerns*, *supra* note 5; Misra, *Who's Tracking Your License Plate?, supra* note 3 ; Hodnett Testimony at 192-194.

[7] *See* R.A. at 59-64.

[8] *See, e.g.*, R.A. at 65 (noting GPS coordinate for the scan at Latitude -41.743872 by Longitude -70.586903); *Decimal degrees*, Wikipedia, https://en.wikipedia.org/wiki/Decimal_degrees (noting at six decimal places, GPS coordinates are accurate to within 43-111 mm and precise enough to recognize individual humans).

[9] *See* ELSAG North America, *Mobile Plate Hunter–900*, DuraTech USA, https://www.duratechusa.com/Products/MPH900.htm.

trips."[10] In Los Angeles, the Police and Sheriff's Departments together collect data on 3 million cars every week,[11] while the City of Atlanta processes nearly 30 million plates each month using just 347 ALPR cameras.[12] As the Boston Globe noted in 2013, "[e]ven smaller departments such as Fitchburg scan 30,000 plates per month with just one license-reading system, easily 10 times more than an officer could manually check."[13]

What is more, ALPR use by government agencies is increasing rapidly. In 2013, the federal Bureau of Justice Statistics found that 93% of police departments in cities with 1 million or more people, as well as more than three-quarters of departments serving 100,000 or more residents, used their own ALPR systems.[14] A 2014 nationwide survey of law enforcement ALPR use noted

---

[10] Matt Rocheleau, *The State Police know every time you drive on or off Cape Cod*, The Boston Globe (Apr. 6, 2019) https://www.bostonglobe.com/metro/2019/04/06/the-state-police-know-every-time-you-drive-off-cape-cod/ydJthj2DQYn6TKcstpPYYM/story.html.

[11] See Jennifer Lynch & Peter Bibring, *Secrecy Trumps Public Debate in New Ruling On LA's License Plate Readers*, EFF (Sept. 3, 2014), https://www.eff.org/deeplinks/2014/09/secrecy-trumps-public-debate-new-ruling-las-license-plate-readers; Aaron Mendelson, *California Police Scanned More Than 1 Billion License Plates—Rarely Finding Cars On 'Hot Lists'*, LAist (Nov. 16, 2018) https://laist.com/2018/11/16/license_plate_readers_eff_analysis.php.

[12] Josh Wade & Aaron Diamant, *Eyes on the Road*, Atl. Journal-Constitution, http://specials.ajc.com/plate-data/.

[13] Shawn Musgrave, *Big brother or better police work? New technology automatically runs license plates . . . of everyone*, Boston.com (Apr. 9, 2013), https://www.boston.com/news/local-news/2013/04/09/big-brother-or-better-police-work-new-technology-automatically-runs-license-plates-of-everyone.

[14] Brian A. Reaves, *Local Police Departments, 2013: Equipment and Technology* at 4, U.S. Dep't of Justice, Bureau of Justice Stat. (July 2015), https://www.bjs.gov/content/pub/pdf/lpd13et.pdf.

"[A]LPR acquisition has most likely tripled" in the previous ten years.[15] And according to EFF and Muckrock's recent national survey, 173 law enforcement agencies scanned a total of 2.5 billion license plates in 2016 and 2017.[16]

This location information can be shared among local, state, and federal agencies, as well private companies, through regional, state-wide, and even national databases. In this case, the Executive Office of Public Safety and Security (EOPSS) shared ALPR location records with the Barnstable Police. And other agencies in Massachusetts are sharing and pooling their data as well. For example, in 2013, a federal-state fusion center teamed up with Vigilant Solutions, a private company and one of the largest aggregators of ALPR data in the country, to create a "regional ALPR network consisting of 22 ALPR systems in the surrounding Boston area and over 30 systems across the Commonwealth of Massachusetts."[17] Each system was composed of numerous ALPRs. Collected data is also shared with the Department of Homeland Security and the FBI. In addition agencies that share their data with Vigilant not only have

---

[15] Cynthia Lum et al., *The Rapid Diffusion of License Plate Readers in U.S. Law Enforcement Agencies* at 10, Ctr. for Evidence-Based Crime Pol'y, Geo. Mason Univ. (Dec. 2016), http://cebcp.org/wp-content/lpr/LPR-National-Survey-Report-2016.pdf.

[16] Misra, Who's Tracking Your License Plate?, supra note 3.

[17] Ayacht Technology Solutions (ATS) the leading New England integrator for Automated License Plate Recognition Technology (ALPR), Ayacht Technology Solutions (June 20, 2013), http://www.ayacht.com/2013/06/1585/.

access to data collected by other agencies around the country,[18] but also to Vigilant's database of privately collected scans, which currently totals 6.5 billion scans and is growing at a rate of 35 million plate scans a month.[19]

III. Police use ALPRs to obtain location data with little oversight.

Once a license plate is in the database, police can use ALPR systems in a number of ways. For instance, police can create a "hot list" of plates from vehicles they are interested in tracking. ALPR systems will then compare every future scan of a license plate against this list and immediately alert designated officers when that plate is read by an ALPR. Comm. Br. at 13, 15.[20] This location tracking can extend indefinitely without the individual's knowledge. Police also accumulate and store ALPR data for use in future investigations to identify drivers' past movements and locations. Comm. Br. at 13-14.[21] In Massachusetts, EOPSS retains all ALPR records for one year. *Id.*

Massachusetts does not currently regulate the use of ALPR systems by statute. This means that law enforcement agencies set their own policies for who has access to ALPR systems, who may add a plate to a hot list or obtain historical information, and

---

[18] About, Vigilant Solutions, https://vigilantsolutions.com/about.
[19] *Id.*; *see also* Digital Recognition Network, https://drndata.com/ ; *CarDetector – Mobile Hit Hunter*, Vigilant Solutions, https://www.vigilantsolutions.com/wp-content/uploads/PSL_Mobile_Hit_Hunter_MHH_VS.pdf.
[20] See Misra, Who's Tracking Your License Plate?, supra note 3.
[21] *See* Klein & White, *License plate readers: A useful tool for police comes with privacy concerns*, *supra* note 5.

for what purpose. Many agencies in the Commonwealth operate ALPR systems without any policies at all.[22] A 2013 investigation by MuckRock and the Boston Globe found that "[f]ewer than a third of [Massachusetts police agencies] – just 17 out of 53 that use ALPR – have formal, written standards to govern use of their scanners and the plate scan data they collect."[23]

In this case, the Department of State Police General Order Number TRF-11 governs both the operation of the ALPR used on the Sagamore and Bourne bridges, and the Barnstable Police Department's use of ALPR technology during the course of criminal investigations.[24] This policy's guidance is limited to the instruction that it shall be used only in "furtherance of official and legitimate law enforcement operations and public safety."[25] However, beyond this vague statement, it appears that plates may be added to hot lists for nearly any reason at all. Indeed, although the policy describes several examples of situations in which an officer might want to add a plate manually to the system—such as AMBER Alerts, "Be On Look Out (BOLO)," and "Attempt To Locate (ATL)"—it notes that manual entries "should not be limited to" the examples on the list.[26]

---

[22] Shawn Musgrave, *Massachusetts police lack policies for license plate scanners*, Muckrock (Apr. 10, 2013), https://www.muckrock.com/news/archives/2013/apr/10/license-plate-scanners-use-across-massachusetts/.
[23] *Id*.
[24] R.A. at 22-23.
[25] R.A. at 154.
[26] R.A. at 156.

IV. ALPR location data can reveal detailed private and personal details about individuals.

Even a small amount of ALPR data can reveal a person's identity as well as sensitive information about that person. By storing data for long periods of time, ALPR databases allow officers to query months' or years' worth of information about a car's past locations. This allows officers to make inferences about individuals that they could not have made without such historical data. ALPR data can reveal not only where a driver was on a given date and time in the past, but can also suggest where a driver may be in the future.[27] As one regional California agency recognized in its privacy impact assessment, "particularly when collected over an extended period of time," ALPR data "could potentially be misused to infer additional information about an individual that is not relevant to police purposes and potentially sensitive for the individual. Such inferences could include, but are not limited to: non-relevant personal relationships; marital fidelity; religious observance; and political activities."[28]

License plate data is already being used to identify

---

[27] State of New Jersey, *Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data* at 4 (effective Jan. 18, 2011), http://www.state.nj.us/lps/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf; Steve Connor, *Surveillance UK: why this revolution is only the start*, The Independent (Dec. 22, 2005), http://www.independent.co.uk/news/science/surveillance-uk-why-this-revolution-is-only-the-start-520396.html.

[28] Northern California Regional Intelligence Center Initial Privacy Impact Assessment for Automated License Plate Reader Technology at 3, Northern Cal. Reg'l Intelligence Ctr., https://ncric.org/html/NCRIC%20ALPR%20PIA.PDF.

individuals and their personal characteristics and habits. In August 2012, the Minneapolis *Star Tribune* published a map displaying the 41 locations where license plate readers had recorded the mayor's car in the preceding year.[29] In 2018, local reporters in Atlanta were able to use ALPR data to map a vehicle's travels over the course of just one day.[30] Using Oakland Police Department ALPR data, *Ars Technica* was able to correctly guess the block where a city council member lived after less than a minute of research.[31] *Ars Technica* also ran the plate number from a random vehicle near a bar against the Oakland data; it found that "the plate had been read 48 times over two years in two small clusters: one near the bar and a much larger cluster 24 blocks north in a residential area—likely the driver's home."[32] Given these capabilities, is no wonder that the International Association of Chiefs of Police has cautioned that ALPR technology 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."[33]

---

[29] Eric Roper, *City cameras track anyone, even Minneapolis Mayor Rybak*, Star Tribune (Aug. 17, 2012), http://www.startribune.com/local/minneapolis/166494646.html.
[30] Josh Wade, *Follow the trail of a license plate*, Knight Lab, https://uploads.knightlab.com/storymapjs/ca566c1c597556a26043831ed5f47a6d/license-plate-readers/index.html.
[31] Cyrus Farivar, *We know where you've been: Ars acquires 4.6M license plate scans from the cops*, Ars Technica (Mar. 24, 2015, 6:00 AM), http://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops.
[32] *Id*.
[33] *Privacy impact assessment report for the utilization of*

SUMMARY OF ARGUMENT

The resource constraints and limits of traditional surveillance techniques have long guided society's reasonable expectations of privacy in public location information. To ensure that technology does not destroy these baseline privacy standards, both this Court and the United States Supreme Court have held that the use of electronic surveillance to obtain access to information otherwise unknowable via traditional surveillance—including extended-tracking information, historical location information, and instant real-time location information—constitutes a search that triggers the warrant requirement. (pp. 16 - 21).

Much like GPS and CSLI surveillance, ALPRs are capable of obtaining extended-tracking information, historical location information, and instant real-time location information. As a result, the government must obtain a warrant when it uses ALPRs for these purposes. The fifteen-year old *Commonwealth v. Starr* decision, 55 Mass. App. Ct. 590 (2002), where the Appeals Court held that there was no expectation of privacy against the manual inspection of a license plate to check registration, does not address, let alone govern, the constitutional implications of the use of ALPR to track or locate an individual's otherwise unknowable location. (pp. 21 - 31).

Here, the Barnstable police used ALPRs to obtain dozens of

---

license plate readers at 13, Int'l Assoc. of Chiefs of Police (Sept. 2009), https://www.theiacp.org/sites/default/files/all/k-m/LPR_Privacy_Impact_Assessment.pdf.

detailed location records, including at least 128 historical location records spanning a two-month period and at least a dozen real-time alerts, none of which would have been otherwise knowable via traditional surveillance. This use of ALPR constitutes a search under art. 14 and the Fourth Amendment subject to the warrant requirement. (pp. 31 - 33).

ARGUMENT

I. The use of electronic surveillance to collect location information that the government could not obtain through traditional surveillance constitutes a search under art. 14 and the Fourth Amendment subject to the warrant requirement.

"A search in the constitutional sense occurs when the government's conduct intrudes on a person's reasonable expectation of privacy." *Almonor*, 482 Mass. at 40 (cleaned up).[34] To preserve the "degree of privacy against government that existed when the Fourth Amendment was adopted," *Carpenter,* 138 S. Ct. at 2214, both this Court and the United States Supreme Court have held that individuals retain a reasonable expectation of privacy in the types of location information that could not be obtained via traditional surveillance, *see, e.g., id.* at 2217; *Commonwealth v. Rousseau*, 465 Mass. 372, 375 (2013). The government's use of electronic surveillance to collect this kind of information—including extended-tracking information,

[34] Because the motion judge appeared to assume subjective expectation of privacy and move directly to an analysis of an objective expectation of privacy, R.A. at 32-34, this brief will do the same.

historical location information, and instant real-time location information—therefore constitutes a search subject to the warrant requirement. *See Almonor,* 482 Mass. at 37; *Augustine*, 467 Mass. at 254-55; *Rousseau*, 465 Mass. at 382.

A. Art. 14 and the Fourth Amendment protect a reasonable expectation of privacy in public location information that is unknowable via traditional surveillance.

Society's expectation of privacy in information about individuals' location and movements in public has long incorporated the constraints of limited time, resources, and capabilities inherent in traditional surveillance practices. *See, e.g., Commonwealth v. Connolly*, 454 Mass. 808, 834 (2009) (Gants, J., concurring); *Carpenter*, 138 S. Ct. at 2218. Before the computer, "the greatest protections of privacy were neither constitutional nor statutory, but practical;" physical surveillance of any significant duration was so "difficult and costly" that it was "rarely undertaken." *Jones*, 565 U.S. at 429 (Alito, J., concurring).

Technological advances have now provided police officers with "extraordinarily powerful surveillance tool[s]" that have "no analog in the traditional surveillance methods of law enforcement[.]" *Almonor,* 482 Mass. at 46. Gone are the checks and balances that previously limited the government's ability to track or find an individual. In response, 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,* 482 Mass. at 41 (cleaned up); *see also Carpenter*, 138 S. Ct. at 2223 (urging courts to remain vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections").

Thus, this Court has determined that the government may use technology to monitor individuals' movements in public "*to the extent that the same result could be achieved through visual surveillance"* without intruding on their reasonable expectations of privacy. *Augustine,* 467 Mass. at 252 (emphasis added). Under such circumstances, electronic surveillance will not undermine the core privacy protections that have existed since the enactment of art. 14. But where the government's use of technology to track or find an individual's location exceeds the limits of traditional surveillance and provides access to "a category of information otherwise unknowable," it intrudes upon a reasonable expectation of privacy, and triggers the warrant requirement. *Almonor*, 482 Mass. at 46 (quoting *Carpenter*, 138 S. Ct. at 2218); *see also Connolly*, 454 Mass. at 822 (noting "despite the increasing use of sophisticated technological devices, there has not been a corresponding societal expectation that government authorities will use such devices to track private citizens"). To hold otherwise "would undoubtedly shrink the realm of guaranteed privacy under art. 14 and leave legitimate privacy rights at the mercy of advancing technology." *Almonor*, 482 Mass. at 47.

B. The government's use of electronic surveillance to obtain extended-tracking information, historical location information, or instant real-time location information otherwise unknowable via traditional surveillance triggers the warrant requirement under art. 14 and the Fourth Amendment.

Over the past decade, this Court has identified at least three categories of location information "otherwise unknowable" via traditional surveillance that require a warrant to obtain via electronic surveillance. The underlying decisions, which involve either GPS or CSLI surveillance, all turn on the fact that the type of location information at issue would have been unattainable via traditional surveillance. *See, e.g., Almonor*, 482 Mass. at 44 n13, 46; *Augustine*, 467 Mass. at 254; *Rousseau*, 465 Mass. at 382.

First, this Court has held that the government's use of electronic surveillance to track an individual's location over an extended period—measured in days, not months or years—triggers the warrant requirement. *See, e.g., Rousseau*, 465 Mass. at 382 (using GPS to track a car for thirty one days required a warrant); *Connolly*, 454 Mass. at 835 (using GPS to track a car for fifteen days required a warrant). Before recent technological innovations, individuals could reasonably expect that the government would not monitor their movements over the course of several days because physical surveillance was costly, labor intensive, and imprecise. But electronic surveillance "is detailed, encyclopedic, and effortlessly compiled." *Carpenter*, 138 S. Ct at 2216. It cheaply "provides an all-encompassing record" of an individual's whereabouts, opening "an intimate

window into a person's life" that reveals "not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." *Id.* at 2217-18 (cleaned up). Police could not typically expend the resources necessary to obtain this type of detailed information via physical surveillance. Because electronic surveillance eliminates this inherent limitation, the government's use of such technology to collect extended-tracking information invades a reasonable expectation of privacy.

Second, this Court has held that the government's use of electronic surveillance to obtain historical location information triggers the warrant requirement. *See Commonwealth v. Estabrook,* 472 Mass. 852, 858 (2015) (obtaining more than six hours of historical cell site location information required a warrant); *Augustine*, 467 Mass. at 254 (obtaining at least two weeks of historical cell site location information required a warrant); *see also Carpenter,* 138 S. Ct. at 2217-18. Electronic surveillance allows 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." *Augustine*, 467 Mass. at 254 (emphasis in original). Indeed, electronic surveillance is akin to a time machine that allows police to "reconstruct" an individual's past movements, something that is entirely impossible without the aid of technology. *Carpenter*, 138 S. Ct. at 2218. Searching this retrospective data "gives police access to a category of information otherwise unknowable," and

therefore triggers the warrant requirement. *Id.*

Third, this Court has held that the government's use of electronic surveillance to obtain an individual's real-time location information triggers the warrant requirement. *See Almonor*, 482 Mass. at 46-47. "The ability of the government to know where anyone is at any moment poses a profound threat to the right to be let alone." *Id.* at 55 (Lenk, J., concurring). Without technology, the police cannot instantly locate any person at any time. Instead, traditional surveillance requires that at least one officer physically find an individual to begin tracking. Resource constraints limit the ability of police to physically locate every person. Not so with electronic surveillance, which allows police to cheaply and easily pluck a person's precise location out of thin air. The power to do so without judicial oversight "is far too permeating and too susceptible to being exercised arbitrarily by law enforcement – precisely the type of governmental conduct against which the framers sought to guard." *Id.* at 46-47 (cleaned up).

II. The use of ALPRs to obtain location information that the government could not obtain through traditional surveillance constitutes a search under art. 14 and the Fourth Amendment subject to the warrant requirement.

As described above, this Court has already held that the government's use of GPS or CSLI surveillance to search otherwise unknowable location information implicates a reasonable expectation of privacy. But these decisions are not anchored to the particular type of technology used to conduct surveillance; they focus instead on the type of information collected via that

technology. *See, e.g., Almonor*, 482 Mass. at 46 (acknowledging "society's expectation has been that law enforcement could not secretly and instantly identify a person's real-time physical location at will" given the resource constraints of traditional surveillance to collect this information); *Augustine*, 467 Mass. at 254 (holding a reasonable expectation of privacy attaches to historical location information because this "category of information" was not available via traditional surveillance); *Rousseau*, 465 Mass. at 379-80, 382 (adopting conclusion that a person has a reasonable expectation of privacy against extended location monitoring given the resource constraints of traditional surveillance to collect this information). Because ALPRs are capable of revealing the same types of otherwise unknowable information, the government must obtain a warrant when they are used for those purposes.

A. Using ALPRs to obtain extended-tracking information constitutes a search under art. 14 and the Fourth Amendment subject to the warrant requirement.

Much like GPS or CSLI, ALPRs can generate detailed location information about an individual over an extended period of time. The Massachusetts State Police have acknowledged that that there are ALPRs "throughout" the Commonwealth.[35] According to EOPSS, as of 2015 there were at least 168 license plate readers in

[35] Matt Rocheleau, *The State Police know every time you drive on or off Cape Cod*, The Boston Globe, April 6, 2019 https://www.bostonglobe.com/metro/2019/04/06/the-state-police-know-every-time-you-drive-off-cape-cod/ydJthj2DQYn6TKcstpPYYM/story.html.

Massachusetts.[36] Significant decreases in the cost of this technology over the past three years may have driven this number even higher.[37] Capturing up to 1,800 plate reads per minute,[38] these readers capture and deposit millions of records into databases.[39] Indeed, the ALPRs on the Bourne and Sagamore bridges alone have recorded "more than 100 million trips."[40]

Each ALPR scan contains detailed location information, including precise time, date, lane and direction information, along with a photograph of the license plate. *See* R.A. at 59-100. Using ALPRs to track an individual over an extended period of time therefore produces exactly the type of previously unknowable information that triggers the warrant requirement. *Cf.* R.A. at 34 (noting potential strength of art. 14 argument against the use of all ALPR cameras in the Commonwealth "to constructively monitor and catalogue every single movement of an

---

[36] Executive Office of Public Safety and Security, Response to Public Records Request (July 24, 2015), https://data.aclum.org/wp-content/uploads/2018/06/Rossman-7.24.15.pdf.

[37] Josh Kaplan, *License Plate Readers are Creeping into Neighborhoods Across the Country*, Slate (July 10, 2019), https://slate.com/technology/2019/07/automatic-license-plate-readers-hoa-police-openalpr.html (noting "sudden affordability" of ALPRs and the resulting increase of use of the technology).

[38] *See* ELSAG North America, *Mobile Plate Hunter–900*, DuraTech USA https://www.duratechusa.com/Products/MPH900.htm.

[39] Executive Office of Public Safety and Security, Response to Public Records Request (July 24, 2015) *https://data.aclum.org/wp-content/uploads/2018/06/Rossman-7.24.15.pdf*. EOPPS reported that the number of records held on the date of the request totaled more than fourteen million.

[40] Matt Rocheleau, *The State Police know every time you drive on or off Cape Cod*, The Boston Globe (April 7, 2019) https://www.bostonglobe.com/metro/2019/04/06/the-state-police-know-every-time-you-drive-off-cape-cod/ydJthj2DQYn6TKcstpPYYM/story.html.

individual's car for a very long period").

The District Attorney's suggestion that police do not need a warrant to track an individual using ALPRs because it does not produce a "treasure trove" of information comparable to CSLI or GPS surveillance misses the mark. Comm. Br. at 35. Even the FBI has recognized that ALPRs impact individuals' privacy rights.[41] Although ALPR systems may sometimes compile fewer individual data points than GPS tracking or CSLI, the ubiquity and precision of the readers described above still generate significant volumes of sensitive information about an individual's life. ALPR systems can be used to scan and record vehicles at a lawful protest or house of worship,[42] gather information about certain neighborhoods[43] or organizations, or compile detailed information about travel habits.

It is therefore no surprise that two state Supreme Courts have recently emphasized the privacy implications of ALPR surveillance. In 2017 the California Supreme Court recognized that ALPR data "could potentially reveal where [a] person lives, works, or frequently visits," *ACLU Found. v. Superior Court*, 3

---

[41] *See generally* Kim Zetter, *Even the FBI Had Privacy Concerns on License Plate Readers*, Wired (May 15, 2015), https://www.wired.com/2015/05/even-fbi-privacy-concerns-license-plate-readers.

[42] *See* Adam Goldman & Matt Apuzzo, *With cameras, informants, NYPD eyed mosques*, Associated Press (Feb. 23, 2012), https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques.

[43] *See* Paul Lewis, *CCTV aimed at Muslim areas in Birmingham to be dismantled*, The Guardian (Oct. 25, 2010), http://www.guardian.co.uk/uk/2010/oct/25/birmingham-cctv-muslim-areas-surveillance.

Cal. 5th 1032, 1044 (Cal. 2017), while the Virginia Supreme Court held last year that photographs and data associated with license plate scans constitute "personal information" under the state's data privacy law that "afford a basis for inferring [an individual's] personal characteristics[.]" *Neal v. Fairfax Cty. Police Dep't*, 295 Va. 334, 346–47 (2018). As these decisions suggest, a person can reasonably expect to be protected from extended ALPR surveillance without judicial oversight.[44]

B. Using ALPRs to access historical location information constitutes a search under art. 14 and the Fourth Amendment subject to the warrant requirement.

ALPRs also enable the police to recreate an individual's location history weeks or even months later. "In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." *Carpenter*, 138 S. Ct. at 2218. Now, much like CSLI and GPS, ALPRs allow the police to "travel back in time to retrace a person's whereabouts, subject only to the retention policies" of the database. *Id*. Here in Massachusetts, EOPSS retains any information captured by the ALPR system for one year. Comm. Br. at 13-14. This ability to recreate an individual's movements up

[44] The District Attorney's argument that "the duration of surveillance is only relevant if the defendant had a reasonable expectation of privacy," Comm. Br. at 40, turns this Court's jurisprudence on its head. Individuals' *already* possess a reasonable expectation of privacy that their "comings and goings will not be continuously and contemporaneously monitored except through physical surveillance," which is implicated by electronic surveillance's ability to easily and cheaply compile extended tracking information. *Connolly*, 454 Mass. at 835 (Gants, J., concurring).

to 12 months prior triggers a reasonable expectation of privacy that necessitates a warrant. *Cf. Carpenter*, 138 S. Ct. at 2217 (requesting six-month old location information violated a reasonable expectation of privacy);[45] *Augustine*, 467 Mass. at 233-34 (requesting month-old location information violated a reasonable expectation of privacy).

C. Using ALPRs to obtain instant real-time location information constitutes a search under art. 14 and the Fourth Amendment subject to the warrant requirement.

Finally, ALPRs' hot list alerts provide the government with instant, real-time location information that could not be obtained via traditional surveillance. Once an officer enters a license plate number onto a hot list, the system automatically sends an alert to every designated officer within seconds after that plate is read by an ALPR. This alert includes an image of the license plate, the precise date, time and direction at the time of detection, the site of the camera, and its longitude and latitude coordinates. R.A. at 65-101. These coordinates can place vehicles at specific locations at specific times, locating an individual's car with even more precision than the cell phone data at issue in *Carpenter* or the GPS tracker in *Jones*. *See Carpenter*, 138 S. Ct. at 2218 (CSLI accurate to within one-eighth to four square miles); *Jones*, 565 U.S. at 403 (GPS device accurate to within 50 to 100 feet); *supra* note 8 (ALPR location

[45] The lower court in *Carpenter* noted that in May and June 2011, the government requested information from December 2010. *United States v. Carpenter,* No. 12-20218, 2013 WL 6385838 at *1 (E.D. Mich. Dec. 6, 2013).

data accurate to within 2-4 inches of the camera and within feet of the vehicle).

Just as "society would certainly not expect that the police could, or would, transform a cell phone into a real-time tracking device without judicial oversight," *Almonor*, 482 Mass. at 46, the use of ALPRs to do the same to a car similarly triggers the warrant requirement. To hold otherwise would require individuals to stop driving entirely "just to assure privacy from governmental intrusion," *id.* at 47, which is all but impossible for those who live in parts of Massachusetts where driving is "indispensable to participation in modern society," *Carpenter,* 138 S. Ct. at 2210.

The District Attorney attempts to distinguish this Court's decision in *Almonor* by stating that there, the government "ping[ed]" the individual's cellphone, and here, ALPRs send no such signals to the license plate. Comm. Br. at 37-38. He argues there is no reasonable expectation of privacy because hot list information could instead be obtained via traditional surveillance if an officer stood at the same location as the ALPR, took photographs and notified other officers. *Id.*

But police generally have not, will not, and cannot conduct such labor-intensive traditional surveillance. *Almonor* itself recognized this reality. Although the decision described the government's actions in that case as a "manipulat[ion]" of the defendant's cell phone, 482 Mass. at 44, it also indicated that the amount of effort it would take to obtain location information via traditional surveillance instead of electronic

surveillance is constitutionally significant. 482 Mass. at 46-47.[46] Illustrating this principle, the government action that *Almonor* suggested would *not* implicate a reasonable expectation of privacy was a police officer "who would care to look" in the direction of an individual on a public sidewalk. *Id.* at 42 n11. In contrast, *Almonor* detailed that locating an individual on-demand traditionally required officers "to patrol streets, stake out homes, interview individuals, or knock on doors." *Id.* at 46. "For this reason," the Court explained, "society's expectation has been that law enforcement could not secretly and instantly identify a person's real-time physical location at will." *Id*.

Yet that is exactly what ALPRs' hot list alerts enable. Logistical constraints prevent police from physically surveilling every location 24 hours a day, 7 days a week, 365 days a year. ALPRs effectively do this with almost no effort at all. Thus, while ALPRs do not send a signal to the license plate, they still convert it into a tool that can and does instantly locate the driver's otherwise unknowable real-time location. *Cf. id.* at 59-60 (Lenk, J., concurring) (noting "[i]t is in obtaining an individual's real-time location information that the government interferes with his or her reasonable expectation of privacy"). Given the need to "establish a constitutional jurisprudence that can adapt to changes in the

[46] Grounding its reasoning in the reasonable expectation of privacy rather than seizure doctrine, 482 Mass. at 44 n14, the majority also noted that "[n]othing in our decision suggests that a search only occurs when the government manipulates one's property," *id.* at 47 n15.

technology of real-time monitoring," *Connolly*, 454 Mass. at 836 (Gants, J., concurring)(quoted in *Almonor*, 482 Mass. at 41), the use of ALPRs for this purpose must also trigger the warrant requirement. *Cf. Almonor*, 482 Mass. at 60 (Lenk, J., concurring) (noting that obtaining instant real-time location information, "however accomplished, exceeds the level of intrusion which society is willing to accept from its government").

D. *Commonwealth v. Starr* does not support the proposition that ALPRs can be used to obtain otherwise unknowable location information without a warrant.

The past decade of this Court's jurisprudence indicates that the government's use of ALPRs to obtain otherwise unknowable location information triggers a warrant requirement. Contrary to the District Attorney's suggestion, the Appeals Court's 15-year old decision in *Commonwealth v. Starr* does not suggest otherwise. 55 Mass. App. Ct. 590 (2002); *cf.* Comm. Br. at 32. There, the court held that no warrant was required to run a license plate number through the Law Enforcement Agency Processing System to determine whether the plate was attached to the proper car. *Id.* at 591. For at least three reasons, this holding does not support the District Attorney's argument here.

To begin, *Starr* rested on the now-repudiated principle that "[s]ocietal beliefs, reflecting our common sense, undoubtedly support the conclusion that it is unreasonable to claim privacy in that which one consciously places in public view." *Id.* at 593. As the cases above make clear, both this Court and the United States Supreme Court now agree that a "person does not

surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter*, 138 S. Ct. at 2217; *see also Rousseau*, 465 Mass. at 382. In addition, *Starr* involved a traditional form of surveillance—manual inspection of a license plate—as opposed to the use of any technology. The same cases above also indicate that the latter can trigger constitutional concerns even when the former does not.

Finally, the government conduct at issue in *Starr* involved using a license plate to determine a car's registration. Thus, "the information conveyed [] was central" to the "primary purpose" of license plates to identify cars. *Cf. Augustine,* 467 Mass. at 250 (explaining no reasonable expectation of privacy in number dialed on a phone because this information "was central to the subscriber's primary purpose for owning and using the cellular telephone: to communicate with others"). In contrast, providing a cheap and effective method to comprehensively track a car's location "has no connection at all to the reason" people have license plates. *Cf. id.* (holding individuals maintain a reasonable expectation of privacy in CSLI which "has no connection at all to the reason people use cellular telephones"). The Appeals Court's conclusion that an individual has no expectation of privacy against an officer's use of a license plate to determine the car's registration need not, and indeed does not, extinguish an expectation of privacy against an officer's use of that same license plate to determine the car's

otherwise unknowable location information.[47]

III. The use of ALPRs to obtain Mr. McCarthy's location information constituted a search under art. 14 and the Fourth Amendment subject to the warrant requirement.

Because the Barnstable police used ALPRs to obtain information about Mr. McCarthy's location that was unknowable via traditional surveillance techniques, they needed a warrant to do so. This Court need not now decide whether there is a de minimis use of ALPRs that would not implicate a reasonable expectation of privacy. *Cf. Estabrook*, 472 Mass. at 858 (no warrant required for six hours or less of historical CSLI). Here, the Barnstable police conduct—using ALPRs to obtain two months of historical location records and receive at least a dozen real-time alerts—crossed any such possible threshold.

The District Attorney argues the police did not need a warrant because the ALPR location information was not comparable to that which could have been revealed by CSLI. Comm. Br. at 28. To make this argument, he both underestimates the quantitative

[47] Even if the initial collection and retention of ALPR location data did not trigger a reasonable expectation of privacy—though it does—this would not insulate a further query of that enormous database of location information from the warrant requirement. *See, e.g., Skinner v. Railway Labor Executives Ass'n*, 489 U.S. 602, 616 (1989) (disaggregating initial physical collection of a blood or breath sample from secondary search through "ensuing chemical analysis of the sample to obtain physiological data"). A warrant may be required to conduct later searches of even lawfully collected data. *See, e.g., United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) (requiring investigating agents to obtain a new warrant before searching computer hard-drives that had been lawfully seized pursuant to an earlier warrant). That is especially true where, as here, the search entails a review of voluminous records that were initially collected without any suspicion of wrongdoing.

and qualitative nature of the ALPR location information collected and largely ignores that historical reconstruction and instant real-time tracking provide additional basis for the warrant requirement here.

The District Attorney describes Barnstable's use of ALPRs as revealing that the car "made same-day round trips over the Bourne or Sagamore bridges on at least 21 separate dates." Comm. Br. at 15. But this description masks that the police used ALPRs to obtain 155 separate location records—including both historical and real-time location records—each of which included detailed time, date, location, direction and lane information. R.A. Ex. 2 & 3. Although these records were collected from two fixed points, those points represent the only way to enter or exit Cape Cod by car. Because they enabled the police to know whether Mr. McCarthy was, or was not, on the Cape, the more than twelve dozen ALPR records provided sufficient detail to trigger a reasonable expectation of privacy.[48]

What is more, the majority of these records were historical, revealing information that was otherwise impossible

[48] Even if the fact pattern in this case did not violate a reasonable expectation of privacy—which it does—the use of a broader network of ALPR cameras to obtain location information would trigger the warrant requirement. *Cf.* Comm. Br. at 34 (describing "a network of cameras linked together, which conjures images of the interconnected cameras on the streets of London"). Of course, "the rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'" *Carpenter*, 138 S. Ct. at 2218; *see also Augustine*, 467 Mass. at 237 n16. Networked ALPRs are already deployed across the Commonwealth, making it vital that this Court set a clear rule to that protects against the kinds of pervasive monitoring such a network enables.

to reconstruct. As the District Attorney explains, on February 1, 2017, Detective York of the Barnstable police "was directed to ask for 'a couple of months' worth of images." Comm. Br. at 14. This yielded at least 128 detailed historical location records going back two months to December 1, 2016. R.A. Ex. 2. This quantity of historical records exceeds any duration that could be said to be "too brief to implicate [a] person's reasonable privacy interest." *Cf. Augustine*, 467 Mass at 254 (two weeks of historical CSLI exceeds the boundaries of when police would not require a warrant).

Finally, Barnstable police also used ALPR to obtain at least a dozen real-time alerts, instantly notifying police of Mr. McCarthy's exact location and direction on the bridge. R.A. Ex. 3. This kind of information would have only otherwise been available through constant physical surveillance of both bridges, a practical impossibility given resource constraints. "To know that the government can find you, anywhere, at any time is—in a word—'creepy'." *Almonor,* 482 Mass at 55 (Lenk, J., concurring). Separate and apart from the historical records discussed above, Barnstable's power "not merely to track" Mr. McCarthy, "but to locate him" cheaply, easily, and precisely violated his expectation of privacy by providing the police with an unprecedented capability which, without judicial oversight, is prone to abuse. *Jones v. United States*, 168 A.3d 700, 712 (D.C. 2017); *see also Almonor*, 482 Mass. at 46.

CONCLUSION

For the reasons described above, this Court should hold that government use of ALPRs to obtain location information unknowable via traditional surveillance techniques is a search under art. 14 and the Fourth Amendment subject to the warrant requirement. Because the Barnstable police used ALPRs for this purpose in its investigation of Mr. McCarthy without a warrant,[49] the ALPR location information and all evidence collected as a result should be suppressed.

DATE: September 11, 2019 Respectfully submitted,

/s/ Jessie J. Rossman
Jessie J. Rossman (BBO #670685)
Matthew R. Segal (BBO #654489)
American Civil Liberties Union
Foundation of Massachusetts, Inc.
211 Congress Street
Boston, MA 02110
(617) 482-3170
jrossman@aclum.org
msegal@aclum.org

Nathan Freed Wessler (BBO #680281)
Ashley Gorski (*on the brief*)
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org
agorski@aclu.org

SIGNATURES CONTINUED ON NEXT PAGE

[49] The District Attorney does not argue that any warrant exception applies.

Matthew Spurlock (BBO #601156)
David Rangaviz (BBO #681430)
Committee for Public Counsel Services
Public Defender Division
44 Bromfield Street
Boston, MA 02108
617-910-5727
mspurlock@publiccounsel.net
drangaviz@publiccounsel.net

ON THE BRIEF:

Jennifer Lynch (CA 240701)
Andrew Crocker (CA 291596)
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436 9333
jlynch@eff.org
andrew@eff.org

Counsel for Amici

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with Mass. R. App. P. 17 and 20. It is typewritten in 12-point, Courier New font, and complies with the length limit of 20(a)(2)(e) because it was produced with monospaced font and has 34 non-excluded pages.

/s/ Jessie J. Rossman
Jessie J. Rossman

AFFIDAVIT OF SERVICE

I, Jessie J. Rossman, counsel for the ACLU of Massachusetts, Inc., do hereby certify under the penalties of perjury that on this 11th day of September, 2019, I caused a true copy of the foregoing document to be served by electronic email on the following counsel:

Michael D. O'Keefe
Elizabeth Anne Sweeney
Office of the District Attorney/Barnstable
3231 Main Street
PO Box 455
Barnstable, MA 02630
ESweeney@massmail.state.ma.us

Paul Alan Bogosian
191 Main Street
P.O. Box 288
Wareham, MA 02571
bogoesq@comcast.net

/s/ Jessie J. Rossman
Jessie J. Rossman

No. SJC-12750

COMMONWEALTH,
Appellee,

v.

JASON MCCARTHY,
Appellant.

ON APPEAL FROM A JUDGMENT OF THE SUPERIOR COURT

BRIEF AMICUS CURIAE
OF THE AMERCIAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS,INC.,COMMITTEE FOR PUBLIC COUNSEL SERVICES, THE ELECTRONIC FRONTIER FOUNDATION AND THE MASSACHUSETTS ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
