SJC-12952

Commonwealth of Massachusetts
Supreme Judicial Court

COMMONWEALTH

v.

JOSIAH ZACHERY

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

Matthew Spurlock, BBO #601156
David Rangaviz, BBO #681430
Committee for Public Counsel Services
Public Defender Division
44 Bromfield Street
Boston, MA 02108
617-482-6212
mspurlock@publiccounsel.net

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

Oren Nimni, BBO#691821
Lawyers for Civil Rights
61 Batterymarch Street
5th Floor
Boston, MA 02110
617-988-0606
onimni@lawyersforcivilrights.org

Jennifer Lynch (on the brief)
Andrew Crocker (on the brief)
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
415-436-9333
jlynch@eff.org

September, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Treatises

Constitutional Provisions

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21, the American Civil Liberties Union of Massachusetts, Inc. (ACLUM), the Electronic Frontier Foundation (EFF), and Lawyers for Civil Rights (LCR) 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. ACLUM, EFF, LCR, and MACDL do not issue any stock or have any parent corporation, and no publicly held corporation owns stock in ACLUM, EFF, LCR, or MACDL.

The Committee for Public Counsel Services (CPCS) is a statutorily created agency established by G.L. c. 211D, § 1.

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

The accelerating pace of technology makes possible effortless monitoring of one's movements in public. The search here is a case in point: MBTA's Charlie Card system automatically generates a record of passenger travel on public transportation and retains it for over a year. The Commonwealth asserts that the police may search this database at any time, for any reason, without any level of individualized suspicion or judicial oversight. Here, the BPD made a warrantless, open-ended request for Mr. Zachery's passenger location information, which, under the MBTA's retention policy, would have been saved for fourteen months. But unrestricted police access to our digital footprint flies in the face of reasonable expectations of privacy, shaped by the constraints of traditional surveillance techniques. Because MBTA passenger location information allows the police to uncover and reconstruct the mosaic of any passenger's private life, the police must obtain a warrant before searching it.

STATEMENT OF THE ISSUE

On May 29, 2020, this Court solicited amicus briefs on the following question:

> Whether a person has a reasonable expectation of privacy in information relating to his or her use of a public transportation card known as a Charlie Card, or in any data the Charlie Card may contain or generate.

STATEMENT OF INTEREST OF AMICI

The American Civil Liberties Union of Massachusetts, Inc. (ACLUM) is a membership organization dedicated to the principles of liberty and equality embodied in the constitutions and laws of the Commonwealth and the United States. The rights it defends through direct representation and amicus briefs include the right to be free from unreasonable searches and seizures. See, e.g., *Commonwealth v. Mora*, 485Mass. 360 (2020) (amicus); *Commonwealth v. McCarthy*, 484 Mass. 493 (2020) (amicus); *Commonwealth v Almonor,* 482 Mass. 35 (2019) (amicus); *Commonwealth v. Augustine*, 467 Mass. 230 (2014) (direct representation).

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. Norman,* 484 Mass.

330 (2020); *Commonwealth v. Barillas,* 484 Mass. 250 (2020); *Commonwealth v. Almonor*, 482 Mass. 35 (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 *Commonwealth v. Mora*, 485 Mass. 360 (2020), *Commonwealth v. McCarthy*, 484 Mass. 493 (2020), *Carpenter v. United States*, 138 S. Ct. 2206 (2018), *Commonwealth v. Augustine*, 467 Mass. 230 (2014), and *United States v. Jones*, 565 U.S. 400 (2012).

Lawyers for Civil Rights (LCR) is committed to fostering equal opportunity and fighting discrimination on behalf of people of color and immigrants. Our public transit systems are heavily used by low-income individuals and are essential services in communities of color. LCR, therefore, has a strong interest in ensuring that the privacy rights of all residents of the Commonwealth are protected, and in particular, the rights of marginalized communities that make up public transport ridership. LCR regularly submits briefs in criminal matters with a particular focus on the disparate impact of criminal laws and enforcement. See,

e.g., *Commonwealth v. Buckley*, 478 Mass. 861 (2017); *Commonwealth v. Vallejo*, 480 Mass. 1001 (2018); *Commonwealth v. Espinal*, 482 Mass. 190 (2019).

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

I. The MBTA records and retains passenger location information.

The Massachusetts Bay Transportation Authority ("MBTA") is a "political subdivision of the Commonwealth" that owns and operates public transportation services. G.L. c. 161A, § 2. See [Tr.1:133][1] The MBTA has its own police department, authorized by St. 1968, c. 664, to exercise "within the territorial limits of the authority, the powers and duties conferred or imposed upon police officers of cities and towns."

The rapid transit system (Red, Orange, Blue, Green lines, and Mattapan high-speed trolley) accounts for 60 % of MBTA trips, with average weekday ridership of 779,114 passengers carried by 651 vehicles making stops at 127 stations.

---

[1] The Record Appendix is cited as [R#]. The transcript is cited as [T.I] (2016/11/29) and [T.II] (2017/03/03). The Commonwealth's brief is cited as [CB].

State of the System Report, Rapid Transit at 5, 7, 8, 16 (Dec. 2015), https://perma.cc/3QTF-ET8P. The MBTA's 170 bus routes make up 30% of trips, with average weekday ridership of 446,700 passengers on 991 buses. State of the System Report, Bus at 5, 8, 13 (Dec. 2015), https://perma.cc/39P5-A5YY.

A. The MBTA records and retains location information as passengers "tap" into stations, buses, and trolleys.

The Charlie Card is the MBTA's "electronic fare media." MBTA, Privacy Policy (Dec. 15, 2006), https://perma.cc/V64R-23WR ("Privacy Policy").[2] Three-quarters of MBTA passengers use Charlie Cards to access public transportation. Metropolitan Planning Organization, MBTA 2015-17 Systemwide Passenger Survey at 38 (May 2018) ("Passenger Survey"), https://perma.cc/VHA4-LZR2. Each Charlie Card is assigned two unique identifying numbers: (1) the serial number of the chip "inside the Charlie Card" and (2) the sequence number of the card. [T.11: 155-157][3] The sequence number on general public Charlie Cards begins with the letter "G." [Tr.II:158] On student cards, like Zachery's, the unique sequence number begins with "M." [T.II:158] Each time a passenger uses a Charlie Card, "the MBTA system collects information about the location of the use." [T.II:177; Privacy

---

[2] See Privacy Policy § 16.6 ("'Electronic Fare Media' means a Smart Card or magnetic stripe ticket designed to be used by Customers to obtain MBTA transportation services").

[3] The serial number consists of one digit followed by a hyphen and 10 digits. MBTA, Fares FAQ, https://www.mbta.com/fares/faq

Policy at § 4.5] Charlie Cards use radio frequency to register an individual card to "tap targets" at station gates, and the entrance of buses and trolleys. [T.II: 162] "The tap target will read the card" to record its "unique identifier" serial number. [T.II: 162-163] The time, location, and unique Charlie Card serial number identifier of each tap is "marked down in [MBTA] databases" in real time (T-station fare gates) or at refueling (busses). [T.II:162, 182]

MBTA police have a "terminal in their crime office [where] they can log on and put in th[e] unique [Charlie Card serial] number and get a history" of where and when the card was used "for the last 14 months." [T.II:182, 184] The MBTA police have various methods of matching the Charlie Card (via its serial number) with a passenger. For general public Charlie Cards, the "MBTA police can get information from a database as to the bank information of the person who purchased the Charlie Card." [T.II:186] In the case of student Charlie Cards, "the school is charged with keeping track of the cards to specific students for loss protection." [T.II:189]

Regardless of who purchased (or was issued) the Charlie Card, the MBTA police may (as occurred here) link the card's location information to the passenger from whom it was seized by noting the card's serial number and generating "a chronological list of where the card was used and when." [T.I:136]

B. Video surveillance augments passenger location information.

The "ubiquitous" surveillance cameras at MBTA stations, trains, buses, and trolleys enhance the MBTA's capacity to track passenger travel. [T.II:183]MDOT, Policy on MBTA Video Access, Distribution, & Retention (March 20, 2014), https://perma.cc/2EXC-K93M ("Video Policy"); Powers, New Cameras Keep Watch for T, Boston Globe (Feb. 12, 2014) https://perma.cc/772Q-ZF9X. The MBTA police "match" a Charlie Card "transaction" to the stored video footage database by "go[ing] to the general system to see the video cameras at each station on th[e] particular time the card was used." [T.II:183; T.I:132] The combination of the Charlie Card "tap" travel "database" and the video "database" allows the police to both confirm the identity of the passenger using the card, and track that passenger's movements within the MBTA system, from entrance to exit. [R72; T.I:135-137; T.II:187] The MBTA police have access to the MBTA's surveillance video database and are "responsible for all video requests and distribution related to criminal activity." Video Policy at 2. The MBTA retains most surveillance video footage for thirty days. *Id.*

C. Police obtain and use passenger location information without a warrant.

The MBTA police have a dedicated "portal" that allows them "full access" to Charlie Card travel data, [T.II:182] and the "database" of video footage from the entire MBTA system. [T.II:187] This is a "totally separate computer system" from

the one maintained by the MBTA's Automated Fare Collection Department. [T.II:181]

According to the MBTA, there is "[n]o requirement of an administrative order, order of a court, [or] search warrant" before the MBTA police (or other MBTA unit) searches these databases. [T.II:180] Nor do the MBTA police require a warrant before disclosing passenger location information at the request of outside police agencies — such as the Boston Police Department (BPD) here. BPD Detective Philip Bliss testifies that he "never" obtains a search warrant for MBTA passenger location information requested and received from the MBTA police. [T.I:124-125]

The MBTA does not "broadcast" the MBTA police's warrantless access to passenger location information to the public. [T.II:189] Nor does it disclose that the MBTA police search, compile, and transmit passenger location information to outside police agencies upon request, and without a warrant. MBTA Fraud Detection Unit Supervisor Keenan Grogan acknowledged that "the public would probably think that the Charlie Card [is] anonymous when they tap it." [T.II:189] The MBTA's Privacy Policy — which is *not* posted where Charlie Cards are sold — states that "[e]ach time the patron uses the electronic fare media the MBTA system collects information about the location of its use." [Tr.II:177, citing MBTA Privacy Policy § 4.5] It is silent on whether, and how, the MBTA shares passenger history with police.

II. The police seize Zachery's Charlie Card and search his passenger location information.

A. The police put the Charlie Card seized from Zachery to investigative use.

In the course of investigating a shooting, BPD officers seized Zachery and transported him to headquarters for questioning. [R93-94] After BPD Detective Darlene Logoa terminated the interview, Zachery "was placed under arrest and his belongings were seized incident to that arrest." [R96; T.I: 126-127] The seized property included an "MBTA Charlie Card" which Detective Logoa gave to BPD Detective Bliss. [R96, 101]

Detective Bliss "was aware, based on previous police experience, that Charlie Cards could be used with the MBTA, possibly to lead to other evidence." [T.I:119] He knew that "based on the serial number of the Charlie Card" the police could obtain "certain information" from the MBTA including "who the Charlie Card is assigned to" and "the travels of the user on the public transportation." [T.I:120, 124] This information "could also lead to video which could be lined up with the . . . travels of the user" because "the MBTA stations have video at the entry point where people use their Charlie Cards." [T.I:120, 124]

Detective Bliss observed that the Charlie Card seized from Zachery was a student Charlie Card. [T.I:120] The card had two numbers: "one with a lot of numbers ending in 2752, the other with the letter M and then a series of numbers ending in 4272." [Tr.I:121] Detective Bliss has "several" "police source[s]" at the MBTA that "assist" with MBTA passenger location information searches,

including "detectives, sergeant detectives, lieutenant detectives." [Tr.I:127, 128] He "contacted [Detective] Gillespie of the MBTA" for "assistance in determining what information they had from the card." [Tr.I:121; R101] Detective Bliss provided the MBTA detective with both of the "long number[s]" and "asked if he could give [him] some information" on its use. [Tr.I:121, R121, R128] When asked, Detective Bliss agreed that his request was "open-ended." [T.I:132] He did not ask MBTA Detective Gillespie to "limit the information in any way," nor did he indicate whether he was interested in "any particular time frame." [Tr.I:130]

Detective Bliss did not seek a warrant before examining the seized Charlie Card and "reading the information off it to the MBTA police for them to look for more information." [Tr.I:122]

B. The police search Zachery's passenger location information without a warrant.

BPD's Detective Bliss's request to the MBTA Detective Gillespie bore fruit. [T.I:132] Using the numbers provide by Detective Bliss, "the MBTA police were able to check the activity and able to download MBTA surveillance video of the person using the card." [T.I:134]

At the motion hearing, Detective Bliss did not "recall" the scope of the passenger location information received from the MBTA police in response to his "open ended" request. [T.I:132, 134, 137] He thought it "may have" gone back a year. [T.I:132, 134, 137] Detective Bliss's affidavit in support of the warrant to search

Zachery's cellphone, written six days after he requested the passenger location information from the MBTA police, describes surveillance on at least two dates: February 11, 2015 (the date of the arrest) and January 26, 2015. [R71-72, 101]. Detective Bliss averred that this location information, compiled by MBTA detectives "able to check the activity on that card" and "able to download MBTA surveillance video that shows video of the person using that card" yielded "several video and still photos of the person who is using that particular card on various dates." [R71][4] Using the Charlie Card location information and "matching" video, he learned that on February 11, Zachery took the Orange Line from Jackson Square, got off at Forrest Hills towards the busway, walked back and forth in and immediately outside the station while using his phone, and left the station on the busway side. [R72, T.I:135-137] The video also disclosed that Zachery was wearing the same jacket on January 26 and February 11. [R71-72]

The passenger location information for those two days was "not the only information that [Detective Bliss] obtained from the MBTA." [T.I:137] Rather, those dates "were included in [the affidavit] because" they were "relevant" to establishing probable cause for the search warrant in "this case." [T.I:137]

[4] The MBTA police "were able to look at that video based on the time periods that they had for when the card was used." [T.I:131-132]

Detective Bliss did not seek a warrant for the MBTA "travel history" associated with the card, including the "travels of the user on public transportation" and "video which could be lined up with the travels of the user" that he sought from the MBTA police. [T.I:120, 124]

SUMMARY OF ARGUMENT

I(A). Art. 14 and the Fourth Amendment protect a reasonable expectation of privacy in one's movements in public against "detailed, encyclopedic, and effortlessly" compiled electronic monitoring that exposes the mosaic of one's life. [pp. 20 - 22]

I(B). Under the mosaic theory, the police acquisition of MBTA passenger location information is a search in the constitutional sense, because (among other things) it monitors and retains passenger travel for a significant duration, in many locations, both real-time and historically, is augmented by video surveillance, and proceeds surreptitiously. [pp. 22 - 31]

II. Precedent from this Court and the Supreme Court establish that the third-party doctrine does not shield this location-disclosing information from constitutional analysis. [pp. 31 - 34]

III. Low-income passengers least able to afford alternative modes of transportation are most affected by the police's warrantless acquisition of MBTA passenger location information. This Court has rejected resource-dependent approaches to privacy rights. [pp. 35 - 36]

IV. The search of Zachery's passenger location information was tainted by the investigative use of the Charlie Card seized incident-to-arrest, when BPD Detective Bliss recorded the card's registration and serial numbers for transmission to the MBTA police, without a warrant. [pp. 36 - 37]

ARGUMENT

I. BPD acquisition of MBTA passenger location information is a search under art. 14 and the Fourth Amendment, subject to the warrant requirement.

A. Individuals maintain a reasonable expectation of privacy in the mosaic of their public movements.

"A search in the constitutional sense occurs when the government's conduct intrudes on a person's reasonable expectation of privacy." *Commonwealth v. Almonor*, 482 Mass. 35, 40 (2019). Importantly, "a person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter v. United States,* 138 S. Ct. 2206, 2217 (2018). Instead, "[w]hen 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." *Commonwealth v. McCarthy*, 484 Mass. 493, 502 (2020). That is so because "location information" generated by automatically and electronically "monitoring of one's comings and goings in public places" "provides an intimate window into a person's life." *Almonor*, 482 Mass. at 54, allowing the police to make inferences otherwise impossible without this pervasive digital record.

Increasingly "detailed, encyclopedic, and effortlessly compiled" digital databases of public movements, *Carpenter*, 138 S. Ct. at 2216, have been a "gift to law enforcement," *Augustine*, 467 Mass. at 251. Before widespread computer use, "the greatest protections of privacy" were practical: physical surveillance of significant duration was so "difficult and costly" that it was "rarely undertaken." *United States v. Jones*, 565 U.S. 400, 416 (2012)(Alito, J., concurring). The "overly pervasive police presence" enabled by our digital footprint "undercuts" constitutionally protected privacy rights because it is not bounded by practical constraints that previously limited surveillance, proceeds surreptitiously, and gives the police access to previously unknowable information. *McCarthy*, 484 Mass. at 493.

To address these concerns, and to protect the "degree of privacy against government that existed when the Fourth Amendment" and art. 14 were adopted, *Carpenter*, 138 S. Ct. at 2214, this Court and the Supreme Court have "articulate[d] an aggregation principle for the technological surveillance of public conduct, sometimes referred to as the mosaic theory." *McCarthy* 484 Mass at 503. This approach inquires "whether a series of acts that are not searches in isolation amount to searches when considered as a group." *Id.* at 503 n.10, quoting Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 320 (2012). It considers the "sum of one's public movements" and "ask[s] whether people reasonably expect that their movements will be recorded and aggregated" to draw powerful

inferences not only concerning their whereabouts but their private lives. *Id.* at 504, quoting *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). Relevant factors include the duration of the surveillance, and whether it is episodic or continuous, provides real time data, and aggregates "massive amounts of data electronically that otherwise would be difficult, if not impossible for a human to compile and analyze." *Commonwealth v. Mora*, 485 Mass. 360, 369 n.10 (2020).

Under this analysis, the MBTA passenger location information generated for the Boston police "amounted to a search" in the constitutional sense. *Id.*

B. The BPD's warrantless acquisition of MBTA passenger location information violates constitutionally protected privacy interests.

The principles above establish that law enforcement must get a warrant before seeking MBTA passenger location information of any significant duration. Acquisition of such data is a search in the constitutional sense because (1) it invades a "subjective expectation in the object of the search," and (2) "society is willing to recognize that expectation as reasonable." *Augustine*, 467 Mass. at 242.[5]

The following factors are salient to the analysis:

---

[5] Zachery attested that he "did not know that the use of the [Charlie Card] generated a record of [his] whereabouts and travel history on the MBTA [and that] he did not consent to the police conducting a search of [his] MBTA travel history that was connected to the use of the [Charlie Card.]" [RA26-27]. No more is required. *Mora*, 485 Mass. at 366.

1. MBTA collects and retains passenger location information for a significant duration.

Like the monitoring of a cellphone user's location when making or receiving calls, *Commonwealth v. Estabrook*, 472 Mass. 852, 854 (2015) (telephone-call cell-site location information (CSLI) over six hours), analysis by the police of every train, bus, or trolley trip is effectively impossible via traditional surveillance.[6]

At the threshold, the "salient consideration is the length of time for which a person's [MBTA passenger location information] is requested, not the time covered by the person's [location information] that the Commonwealth ultimately seeks to use as evidence at trial." *Id.* at 859. See also *McCarthy*, 484 Mass. at 505 (same); *Id.* at 515 (Gants, C.J., concurring). Because BPD Detective Bliss made an "open ended" request to MBTA Detective Gillespie for all the passenger location information "they had from the card," [T1:132, T.1:121] the relevant period is fourteen months, the length of time for which the MBTA retains passenger

[6] The motion judge characterized the search-threshold for telephone-call CSLI as "continuously tracking a person's location over a two-week period." [RA117], citing *Augustine,* 467 Mass. at 230, 255. That is incorrect. Art. 14 requires a warrant for over six hours of telephone-call CSLI. *Estabrook,* 472 Mass. at 859. Telephone-call CSLI is "episodic, not continuous." *Augustine*, 467 Mass. at 266 (Gants, J., dissenting).

location information. [T.II:182][7] *Commonwealth v. Rousseau*, 465 Mass. 372, 376 (2013) (analyzing thirty-one days of GPS monitoring, not data that placed vehicle near suspected crime on four dates).

An "open-ended" [T.I:132] request for fourteen months of the time and place of every trip on public transportation plainly constitutes a search under this Court's precedent. See *McCarthy*, 484 Mass. at 506 (one-year retention "long enough to warrant constitutional protection"). But even if the relevant time period was sixteen days — the period between the January 26 and February 11 trips cited in the warrant application — such monitoring would still be more than sufficient to constitute a search. See *Estabrook*, 472 Mass. at 859 (over six hours episodic telephone-call CSLI). Police acquisition of passenger location information of even sixteen days is effectively impossible via physical surveillance, because it would require surreptitiously tailing the target for the entire period, noting every train, trolley, and bus ride. So extensive an operation would be "difficult and costly and therefore rarely undertaken" outside of the most exceptional circumstances. *Jones*, 565 U.S. at 429, 420 n.3 (Alito, J., concurring). And stationing police officers (or informants) to keep an eye out for the target at every station, bus, and trolley

---

[7] Zachery established the scope of the Boston Police request at the motion hearing. [T.I:137-138; T.II:182] Cf. *McCarthy*, 484 Mass. at 515 (Gants, C.J., concurring) (because the evidence is in the agency's possession, "the agency must preserve the historical locational data . . . that the agency *retrieved* . . . and [the] search request") (emphasis in original).

is beyond the means of all but the most robust police state. Because "the same result" could not "be achieved through visual surveillance.," *Augustine*, 467 Mass. at 252, the duration of the MBTA passenger location information searched here — regardless of whether it is fourteen months or sixteen days — cuts strongly in favor of constitutional protection.

2. MBTA collection of passenger location information is pervasive.

In addition to the *duration* of passenger location information retained by the MBTA and searched by the police, the pervasiveness of MBTA surveillance "reveal[s]" a "substantial picture of an [MBTA rider's] public movements." *McCarthy,* 484 Mass. at 506. The MBTA system includes thousands of "tap points" (bus stops, trolley stops, and train stations) that "register" the time and place of a unique Charlie Card's use to the agency's central computer system (and the MBTA police terminal). *Supra* at 12-14. The "network" of these surveillance points dwarfs the "four [automatic license plate reader (ALPR)] cameras at fixed locations on the ends of two bridges," that failed to meet the search threshold in *McCarthy.* 484 Mass. at 509.[8] The *McCarthy* Court warned, however, that "[i]f deployed widely enough ALPRs" could reveal an individual's location "virtually any time the person decided to drive." *Id.* at 507. That day has already arrived for

[8] ALPRs are "cameras combined with software that allows them to identify and 'read' license plates on passing vehicles." *McCarthy*, 484 Mass. at 494.

MBTA passengers, whose every trip is registered and retained, for real time or historical analysis.

Identifying travel patterns for a particular passenger "could potentially reveal where [a] person lives, works, or frequently visits," *id.* (cleaned up), far more effectively (and accurately) than the four ALPR cameras in *McCarthy*. The time and location of MBTA trips (potentially enhanced by matching video) offers 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).

The "episodic" nature of the Charlie Card "taps" does not change the analysis. Contrary to the motion judge and the Commonwealth, art. 14's protection is not limited to "continuous and contemporaneous" surveillance. [R118, CB61] Rather, law enforcement must obtain a warrant for "location information relating to telephone calls made and received," *Augustine,* 467 Mass. at 862, for a period of greater than six hours. *Estabrook*, 472 Mass. at 853. As the case law makes clear, the fact that MBTA passenger location information (like telephone-call CSLI) is "episodic, not continuous," *Augustine*, 467 Mass. at 266 (Gants, J., dissenting), makes no difference. See *Carpenter*, 138 S. Ct. at 2212 (CSLI "at call origination and call termination").

3. MBTA collects both real-time and historical location information.

Although historical passenger location information is at issue in this case, current technology also permits the MBTA police to monitor real-time travel. This Court has recognized a reasonable expectation of privacy against law-enforcement searches of *both* extended historical location information *and* real-time location information. See *Augustine*, 467 Mass. at 245-55 (historical telephone-call CSLI); *Almonor*, 482 Mass. at 37-39 (one real-time CSLI "ping"). Each method exposes location information that could not be obtained by traditional surveillance. *Carpenter*, 138 S. Ct. at 2217.

With respect to historical passenger location information, "prior to the digital age" discovering a surveillance target's location "for any extended period of time was difficult and costly, and therefore rarely undertaken." *Id.* Moreover, as here, the suspect is usually unknown to the police before they seek to reconstruct a detailed digital trail of his whereabouts. So longer-term historical "tracking" is genuinely novel: "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).

As to real-time location information, the police have never had the ability to pluck an individual's location out of thin air, with no information other than the serial number of his Charlie Card, "virtually any time the person decided to [travel by public transportation]." *McCarthy,* 484 Mass. at 507 ("reasonable

expectation of privacy in one's real-time location"). So "[a]llowing law enforcement to immediately locate an individual" every time he uses the MBTA "contravenes [a reasonable] expectation" of privacy. *Almonor*, 482 Mass. at 46.

4. MBTA surveillance video enhances "tap" passenger location information.

Although the passenger location information derived from Charlie Card tap location information meets the search threshold on its own, searches of surveillance video in the MBTA database "generated" by the "tap" location information, see Solicited Question *supra* at 9 , are an additional, aggregating, factor establishing that the search here violated a reasonable expectation of privacy. The mosaic theory "looks at an aggregated set of data acquisitions [to] determine when they trigger a collective search." Kerr, The Mosaic Theory of the Fourth Amendment at 333. The analysis therefore can consider "different tools," *id.,* used to "target" the object of the surveillance. *Mora*, 485 Mass. at 360.

Here, the police aggregated targeted video from "ubiquitous" cameras to the "tap" registration location information, by "matching" the two databases. [T.II:183] The video searches allowed the police to retrace Zachery's trip from beginning to end. [Tr.I:135-137] Compare *McCarthy*, 484 Mass. at 509 (four ALPR cameras "does not allow" monitoring "even his progress on single journey"). See *Mora*, 485 Mass. at 375 (video "stored digitally, in a searchable format, such that

investigators could comb through it at will").[9] When "combined technologies" are "layered on top of each other . . . the juiced-up surveillance" triggers a constitutional search. Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 Emory L.J. 527, 578-579 (2017).

Mora is not to the contrary. There, the Court declined to infer a reasonable expectation of privacy in "short-term, intermittent, and nontargeted video recording" of the kind "captured by security cameras." 485 Mass. at 369. By contrast, the MBTA video here *was* targeted by "matching" it with Charlie Card tap registration database. [T.II:181, 183] While the surveillance video footage on its own may not be a search, see *Mora* 485 Mass. at 369, here it aggregates into the "collective" of surveillance methods that implicate (and violate) a reasonable expectation of privacy. Kerr at 333-334.

---

[9]Surveillance video technology is increasingly sophisticated: capturing the smallest visual details, enabling rapid and accurate searches, and often coupled with facial recognition technology. See Stanley, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy,* ACLU (2019), https://perma.cc/TFQ2-7FXG. The Court may "take account of more sophisticated systems already in use or development." *Kyllo v. United States,* 533 U.S. 27, 26 (2001). See *Mora*, 485 Mass. at 369 n.10 (factors include possibility of aggregating, impossibility of human to analyze, and level of visual detail).

5. Passengers do not knowingly expose their patterns of travel.

"[E]ven if they are all individually public" a person's travel on the MBTA is "not knowingly exposed in the aggregate." *McCarthy*, 484 Mass. at 504. "Like carrying a cellphone [and] driving" public transportation "is an indispensable part of modern [city] life, one that we cannot and do not expect residents to forgo in order to avoid government surveillance." *Id.* at 507. The Commonwealth's arguments to the contrary are unpersuasive. Cellphone users are also "alert" [CB59] that "cellular telephone technology" requires that a "call connects to a cell site." *Augustine*, 467 Mass. at 250. But that technological fact does not extinguish a reasonable expectation of privacy in over six hours of telephone-call location information. Similarly, a subscriber's ability to "check past [call history] location" [CB59] does not undermine an expectation of privacy in this location information vis a vis the police. The same is true for MBTA passengers. Nor does the Commonwealth provide any support for its assertion that student Charlie Cards are "monitored for abuse" or explain how such monitoring (assuming it exists) undermines an expectation of privacy against the police. [CB59-60]

Of course, the MBTA's Privacy Policy cannot undermine constitutional rights. Cf. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 Berk. Tech. L. J. 1199, 1205 (2009) ("unilateral legislative declaration" insufficient "to undermine constitutional rights"). In any event, the Commonwealth misreads the policy: it allows for "collect[ion] of information

about the location" of Charlie Card use, as might be expected for payment and logistics, Privacy Policy at § 4.5, but it says nothing about whether (or how) "that transaction information may be shared with law enforcement," [CB59] and certainly does not "publicize" its transmission of passenger location information to law enforcement, as the Commonwealth claims. [CB59] To the contrary, MBTA Fraud Detection Unit Supervisor Keenan Grogan acknowledged that passengers "probably think that the Charlie Card [is] anonymous" and testified that the agency does *not* "broadcast" that it shares passenger location information with the police.[10] [T.II:189] Fairly read, the Privacy Policy strengthens, rather than undermines, the reasonable expectation of privacy in one's MBTA passenger location information.

The "factors" the Commonwealth musters to cast doubt Zachery's privacy interest, alone or "in combination," [CB60] fall flat.

II. The third-party doctrine does not apply.

The motion judge relied on cases holding that individuals lack privacy interests in bank records and telephone bills in the possession of "third party"

---

[10] The Privacy Policy's only reference to "shar[ing]" information with other law enforcement agencies occurs in § 4.15, addressing "Pedal and Park Bike Cages." See [Tr.II:178] The "personal information to register to use the Pedal and Park facilities," § 4.15, is not passenger location information.

companies. [R115-116], citing *United States v. Miller,* 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979), to reject any constitutional protection for passenger location information, collected by the MBTA and disclosed to the BPD without a warrant. [R115-117] That doctrine is inapposite to shield police searches of location disclosing information from constitutional scrutiny.

Both this Court and the Supreme Court have declined to "mechanically apply[] the third-party doctrine" to location-disclosing information. *Carpenter*, 138 S. Ct. at 2219. The third-party cases, *Carpenter* explained, "did not rely solely on the act of sharing" but instead, "considered the nature of the particular document sought to determine whether there is a legitimate expectation of privacy concerning their contents." *Id.,* quoting *Miller*, 425 U.S. at 443. Indeed, even before *Carpenter* (and *Augustine*) addressed CSLI, both courts had "shown special solicitude for location information in the third-party context." *Carpenter*, 138 S. Ct. at 2219, citing *Jones*, 565 U.S. at 430 (Alito, J., concurring), *id.* at 415 (Sotomayor, J., concurring). See also *Augustine*, 467 Mass. at 251, citing *Connolly*, 454 Mass. at 835 (Gants, J., concurring). Modern location tracking, this Court explained, is "significant[ly]" different than bank records or telephone numbers. *Augustine*, 467 Mass. 249-251. See *Carpenter*, 138 S. Ct. at 2217 (same). The "seismic shifts in digital technology" from tokens to electronic fare media raise the same concerns with respect to MBTA travel. *Carpenter*, 138 S. Ct. at 2219. And they apply equally to "locational data" allowing "targeted search[es] of locational information"

generated or acquired by law enforcement. *McCarthy*, 484 Mass. at 513 (Gants, C.J., concurring) ("If a law enforcement agency possessed comparable [location] data . . . we would require . . . a search warrant"). See *id.* at 503 (analyzing ALPR data under art. 14).

The digital location information at the MBTA's fingertips — "detailed, encyclopedic, and effortlessly compiled," *Carpenter*, 138 S. Ct. at 2216 — has more in common with CSLI than bank records and telephone numbers. Like CSLI, the passenger location information stored in the MBTA's databases (and available in real time) paints a detailed picture of the passenger's public life, allowing powerful inferences about private affairs. See *supra* at 21 - 32. CSLI and MBTA passenger location information are "linked at a fundamental level" because both "implicate the same constitutionally protected interest . . .[in] a person's movements." *Augustine,* 467 Mass. at 230.

And unlike dialed telephone numbers (*Smith*) or check deposit slips (*Miller*) MBTA's collection and retention of passenger location information "has no connection at all to the reason people use" public transportation. *Augustine,* 467 Mass. at 250. Passengers buy Charlie Cards (or receive them from school) for transportation, not to share "information about their whereabouts with police." *Id.* Passengers do not receive their Charlie Card tap history in a monthly bill. Rather, the transmission of the time and location of a unique Charlie Card's use [Tr.II:162], and the retention of this location information for fourteen months,

[Tr.II:182] "is purely a function" of the MBTA's electronic fare media technology when the passenger embarks on public transport. A*ugustine*, 467 Mass. at 250.

As with CSLI, the police are "not seeking to obtain information provided to [the MBTA] by the defendant" but rather "looking only for a location identifying by-product" of electronic fare media technology, "a serendipitous (but welcome) gift to law enforcement investigations." *Id.* at 251. The reason is simple: passenger location information "yield[s] a treasure trove of very detailed and extensive information about the individual's 'comings and goings' in both public and private places." *Id.* at 251. The concerns about the "rapid expansion" in "data generated through new technologies" that prompted this Court and the Supreme Court to "reconsider the premise" of the third-party doctrine apply fully to MBTA passenger location information. *Id.* at 252 n.35, quoting *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring), *Connolly*, 454 Mass. at 836 n.2 (Gants, J., concurring). This Court should "decline to extend" the third-party doctrine here too. *Carpenter*, 138 S. Ct. at 2217. [11]

---

[11] This Court has not limited its rejection of the third-party doctrine to location-disclosing information that is "continuous and contemporaneous." Contra [R118; CB61]. For example, the doctrine is also inapplicable to "episodic" "location information relating to telephone calls made and received" for a period of greater than six hours. *Augustine,* 467 Mass. at 862; *Estabrook*, 472 Mass. at 853. See *supra* at 23 n.6. MBTA travel data ("taps") are equally "episodic" (and may be just as frequent or infrequent) as telephone-call CSLI. Requiring a warrant for

III. Warrantless searches of MBTA passenger location information burdens those with fewest resources.

Affirming the Superior Court decision would especially impact metro Boston residents with the fewest financial resources. Almost 30 % of MBTA passengers are low income. Passenger Survey at 43.[12] These passengers are the least likely to have access to alternative transportation (vehicles and drivers licenses) to avoid pervasive MBTA surveillance.[13] Discounted student Charlie Cards, like the one at issue here, are a case in point, disproportionately available to low income families.[14] And short of abandoning public transportation altogether (for those with other options) passengers paying cash (or using a single-

---

over six hours of "episodic" telephone-call CSLI, while exempting passenger location information from any constitutional limits under the guise of the third-party doctrine would be incongruous.

[12] The Passenger Survey defines "low income" passengers as those with household incomes of less than $43,500. Passenger Survey at 56.

[13] Low-income passengers account for a disproportionate percentage of MBTA bus travel (41.6%) as compared to rapid transit train (26.5%). Passenger Survey at 56. Almost 40% of bus passengers have no vehicles per household, as compared to 30% of subway passengers. *Id.* at 57. Similarly, only 69% of bus passengers have a valid driver's license, as compared to 82% of train passengers. *Id.*

[14] See MBTA, Middle and High School Student Charlie Cards, https://perma.cc/LD6L-E3W4. Seventy-seven percent of Boston public school students are low income. Kids Today: Boston's Declining Child Population and Its Effect on School Enrollment at 19, Boston Indicators (Jan. 2020), https://perma.cc/H259-Z7LU.

use CharlieTicket) to avoid passenger location information monitoring and retention pay a premium for each trip.[15]

A "resource-dependent approach" to preserving privacy against law enforcement that would "apportion constitutional rights on grounds that correlate with income, race, and ethnicity" is "contrary to the history and spirit of art. 14." *Mora*, 485 Mass. at 367. Allowing warrantless searches of MBTA passenger location information would "undermine . . . long-standing egalitarian principles" *id.*, by putting a price on securing the "privacies of life" from "too permeating a police presence." *Carpenter*, 138 S. Ct. at 2214. Such an outcome would impose a pay-for-privacy escape valve to evade art. 14 and the Fourth Amendment.

IV. The investigative use of a seized Charlie Card requires a warrant.

Property seized incident-to-arrest may be secured "until a valid warrant is obtained." *Commonwealth v. Barillas*, 484 Mass. 250, 254 (2020). Until that time, however, the seized property may not be used "for investigative purposes." Cypher, Criminal Law and Procedure § 5.134 (4th ed. 2014). This rule applies equally to seizures incident-to-arrest, *Commonwealth v. Blevines*, 438 Mass. 604, 609 (2003) (scrutiny of keys seized incident to arrest) and inventory searches, *Commonwealth v. Seng,* 436 Mass. 537, 554 (2002) (account number on bank card).

---

[15] Decosta-Kipa, *MBTA is planning to lower CharlieTicket and cash fares*, Boston.com (May 22, 2020), https://perma.cc/4Y33-EVQE.

There is little question that BPD Detective Bliss made "investigative use" of the seized Charlie Card, *Barillas*, 484 Mass. at 248 , when he noted and transmitted the card's serial and registration numbers ("one with a lot of numbers ending in 2752, the other with the letter M and then a series of numbers ending in 4272") to MBTA Detective Gillespie. [Tr.1:121; R101][16] In *Blevines,* for example, the officers "made investigative use" of seized keys by their "attention" to the keys "to connect the defendant to a particular vehicle." 438 Mass. at 609. And *Seng* held that "read[ing] and record[ing]" of "account numbers on the back" of a bank card that "were not obvious and would not be recalled" tainted the records obtained. *Id.* at 554. See *id.* at 552 ("substantial difference" between observing bank name on card and "examining the card closely enough to comprehend (and record) the multi-digit account numbers"). Because the Charlie Card serial number relayed by Detective Bliss to MBTA Detective Gillespie "led directly" to Zachery's passenger travel history, the evidence should be suppressed. *Blevines*, 438 Mass. at 611.

[16] The numbers were 5-2859812752 and M0014414272. [R71]

Conclusion

The Court should reverse the order approving open-ended and warrantless searches of MBTA passenger location information. The "answer to the question of what police must do before" seeking this pervasive location information "is simple – get a warrant." *Riley v. California,* 573 U.S. 373, 403 (2014).

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

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

Oren Nimni, BBO#691821
Lawyers for Civil Rights
61 Batterymarch Street
5th Floor
Boston, MA 02110
617-988-0606
onimni@lawyersforcivilrights.org

September 21, 2020.

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the Massachusetts Rules of Appellate Procedure that pertain to the filing of briefs and appendices, including, but not limited to those specified in Rule 16(k), 17, and 20. It complies with the type-volume limitation of Rule 20(2)(C) because it contains 6,399 words, excluding the parts of the brief limited by the rule. It complies with the type-style requirements of Rule 20 because it has been prepared in proportionally-spaced typeface using Microsoft Word in 14 point Altheas font.

/s/Matthew Spurlock
Matthew Spurlock

COMMITTEE FOR PUBLIC COUNSEL SERVICES
Public Defender Division
44 Bromfield Street
Boston, Massachusetts 02108
(617) 910-5727
mspurlock@publiccounsel.net
BBO #601156

CERTIFICATE OF SERVICE

Pursuant to Massachusetts Appellate Rule of Procedure 13(c), I certify that on September 21, 2020 I have made service of this Brief upon the attorney of record for each party by Electronic Filing System.

/s/Matthew Spurlock
Matthew Spurlock

COMMITTEE FOR PUBLIC COUNSEL SERVICES
Public Defender Division
44 Bromfield Street
Boston, Massachusetts 02108
(617) 910-5727
mspurlock@publiccounsel.net
BBO #601156