**COMMONWEALTH OF MASSACHUSETTS**

# Supreme Judicial Court

NO. SJC-12890

---

COMMONWEALTH,
RESPONDENT-APPELLEE,

v.

Nelson Mora & others
PETITIONERS-APPELLANTS.

---

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., THE ELECTRONIC FRONTIER FOUNDATION, AND THE CENTER FOR DEMOCRACY AND TECHNOLOGY

---


Matthew R. Segal (BBO 654489)
Jessie J. Rossman (BBO 670685)
Kristin M. Mulvey (BBO 705688)
American Civil Liberties Union
Foundation of Massachusetts, Inc.
211 Congress Street
Boston, MA 02110
(617) 482-3170
msegal@aclum.org
jrossman@aclum.org
kmulvey@aclum.org

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


[*Counsel continued on next page*]

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

Gregory T. Nojeim (DC 398337)
Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, DC 20005
(202) 637-9800
gnojeim@cdt.org

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

### Cases

**Constitutional Provisions**



**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 American Civil Liberties Union (ACLU) is a District of Columbia non-profit membership organization and 501(c)(4) organization. The Center for Democracy & Technology (CDT) is a 501(c)(3) organization incorporated in the District of Columbia. ACLU, ACLUM, EFF, and CDT do not issue any stock or have any parent corporation, and no publicly held corporation owns stock in ACLU, ACLUM, EFF, or CDT.

## 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

This case arises from the Commonwealth's warrantless, months-long use of sophisticated cameras aimed at homes—what the Commonwealth calls "pole cameras"—to surveil everyone who came and went. Police officers could watch the cameras' livestream feed in real time, and remotely angle and zoom close enough to read license plates. App. 104.[1] They could also go back and review the searchable record of this footage at their convenience. *Id.* The Commonwealth argued below, and the Superior Court agreed, that police officers can deploy these home-facing cameras not only against the defendants in this case, but against anyone, at any time, without getting a warrant.

This Orwellian assessment of the Commonwealth's warrantless surveillance authority is inconsistent with the prohibitions against unreasonable searches and seizures in article 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the United States Constitution. Those provisions ensure that technology does not "shrink the realm of guaranteed privacy." *Commonwealth v. Almonor*, 482 Mass. 35, 47 (2019) (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). But digital home-facing pole cameras threaten precisely that. They give police previously unimaginable capabilities to monitor individuals for weeks or months, and to indefinitely store and search this detailed surveillance information.

[1] Citation refers to the Defendants' Appendix.

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 v. United States*, 138 S. Ct. 2206, 2214 (2018) (cleaned up).[2] Because it can enable a "too permeating police surveillance," the Commonwealth's warrantless, long-term use of home-facing cameras violates art. 14 and the Fourth Amendment. *Id.* (cleaned up).

In arriving at this conclusion, it does not matter that home-facing cameras record from a vantage point that is theoretically accessible to the public. In cases involving the government's acquisition of information about individuals' *public* movements, both this Court and the Supreme Court have made clear that individuals can retain a reasonable expectation of privacy in sensitive information even if they have arguably exposed it to the public. See, e.g., *Commonwealth v. Augustine*, 467 Mass. 230, 247-48, 254-255 (2014) (imposing a warrant requirement on the collection of more than two weeks of cell site location information); *Commonwealth v. Rousseau,* 465 Mass. 372, 383 (2013) (holding that extended GPS surveillance of an individual's location in public implicates a reasonable expectation of privacy, explaining "the government's contemporaneous

[2] "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,* ABA For Law Students: Before the Bar (Oct. 3, 2017), https://perma.cc/B2JX-9JSR.; see also Jack Metzler, *Cleaning Up Quotations*, 18 J. App. Prac. & Process 143 (2017).

electronic monitoring of one's comings and goings in public places invades one's reasonable expectation of privacy"); *Carpenter*, 138 S. Ct. at 2217 (imposing a warrant requirement on the collection of more than seven days of cell site location information, explaining "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

The Superior Court concluded that the reasoning of those cases is limited to location tracking, but that is incorrect. App. 120, 123. *Carpenter* held that the Constitution protected an individual's public movements revealed by cell site location information (CSLI) because such information was "detailed, encyclopedic, [] effortlessly compiled" and "deeply revealing." 138 S. Ct. at 2216, 2223. Recognizing that "physical surveillance [] requires a far greater investment of police resources and generates far less information than GPS monitoring," *Rousseau* held there was a reasonable expectation of privacy against extended location tracking via GPS. 372 Mass at 379, 382 (cleaned up). And *Augustine* applied a warrant requirement to CSLI access after acknowledging that it "provide[s] an intimate picture of one's daily life" that can reveal "a broad range of personal ties with family, friends, political groups, health care providers, and others." 467 Mass. at 248 (cleaned up). These conclusions apply with more, not less, force where the Commonwealth effortlessly compiles detailed and deeply revealing information about the comings and goings at someone's home, which is

"first among equals" when it comes to search and seizure protections. *Florida v. Jardines*, 569 U.S. 1, 6 (2013) (cleaned up). The Commonwealth's warrantless, long-term deployment of a home-facing camera therefore violates constitutionally-protected reasonable expectations of privacy.

A contrary conclusion would have at least two deleterious long-term consequences. First, because camera capabilities are constantly evolving, the Commonwealth's deployment of home-facing cameras can be expected to become more intrusive as time passes. The Commonwealth may soon be able to search weeks of footage in seconds, and identify everyone entering or exiting a house via face surveillance algorithms. Second, authorizing warrantless, prolonged pole camera surveillance of a home would disparately impact those with the fewest resources to protect themselves from such monitoring by building walls or using other means. To guard against these outcomes and comport with existing art. 14 and Fourth Amendment jurisprudence, this Court should reverse the Superior Court's denial of the motion to suppress.

## 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 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. Augustine*, 467 Mass. 230 (2014); *Carpenter v. United States*, 138 S. Ct. 2206 (2018); and *United States v. Jones*, 565 U.S. 400 (2012).

The Center for Democracy & Technology (CDT) is a nonprofit public interest organization which seeks to ensure that the human rights we enjoy in the physical world are realized in the digital world. Integral to this work is CDT's representation of the public's interest in protecting individuals from abuses of new technologies that threaten the constitutional and democratic values of privacy and free expression. For twenty-five years, CDT has advocated in support of laws and policies that protect individuals from unconstitutional government surveillance.

This case has profound ramifications that reach far beyond the specific technology at issue, and that threaten the ability to associate, repose, and retreat into one's home.

## STATEMENT OF FACTS

In November 2017, the Massachusetts State Police (MSP), along with the Drug Enforcement Administration (DEA) and several local police departments, began a drug distribution investigation in Peabody and Lynn. App. 64-65. As part of this investigation, the MSP installed four home-facing cameras, including cameras trained on the front of the residences of Nelson Mora and Randy Suarez. App. 102-103.[3] These cameras "recorded without limitation persons coming and going" from these homes. App. 104. Mora and Suarez were "regularly seen" on the footage, as were several other individuals. App. 102-103.

Police officers could view the surveillance footage from a web-based browser in real-time, and remotely control the angle and zoom of the cameras. App. 104. Although the cameras did not "enable[] investigators to see inside any residence," they could zoom close enough to read license plates. App. 104. Officers could also "search and review previously recorded footage." App. 104.

[3] The MSP installed an additional camera that captured the top of a driveway but not any residence. App. 103.

Each of the home-facing cameras were operational for different lengths of the time. For example, the camera trained on Suarez's home operated for two months, while the camera trained on Mora's home operated for nearly five and a half months. App. 102-103. Once the cameras were turned-off, the police transferred the surveillance data onto hard drives for storage. App. 104. Collectively, the video surveillance in this case was produced on a 6-terabyte hard drive. App. 133.

Appellants moved to suppress the warrantless video surveillance as an unreasonable search that violated art. 14 and the Fourth Amendment. Four other individuals indicted in the investigation joined the motion to suppress but did not appeal to this Court. The Superior Court distinguished between individuals whose images were captured on surveillance footage but whose homes were not surveilled (Gregory Inuyama, Lymbel Guerrero, Frantz Adolphe and Aggeliki Iliopoulos), and those whose home were surveilled (Nelson Mora, Randy Suarez and Richard Grullon-Santos).[4]

The Superior Court quickly dismissed the motions of those defendants whose homes were not surveilled, explaining, "an occasional depiction on pole camera footage at another's residence or street is a far cry from continuous video surveillance coverage of one's residence" and does not give rise to "the same

[4] Amici focus their analysis on those defendants whose homes were surveilled.

invasion of privacy and expectation of privacy arguments." App. 114-15. With respect to the motions of those defendants whose homes were surveilled, the Superior Court acknowledged, "homes are a protection at the heart of the fourth amendment and art. 14," and recognized, "a trend has been established to extend constitutional protections against law enforcement surveillance techniques that have evolved through advancements in technology." App. 114, 120. Nevertheless, the Superior Court still denied Mora, Suerez and Grullon-Santos' motions based on its conclusion that the Supreme Court's and this Court's reasoning in its CSLI and GPS tracking cases was "limited to surveillance techniques that track a person's movement's or location." App. 120.

## SUMMARY OF ARGUMENT

1. Individuals need not take extraordinary measures to preserve their subjective privacy interests. As for whether such interests are objectively reasonable, the resource constraints and limits of physical surveillance techniques have long guided society's expectations of privacy. 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 technology to collect detailed information that is effectively unknowable via traditional techniques triggers a warrant requirement. (pp. 18-23).

2. Warrantless, long-term pole camera surveillance of homes violates these standards. Individuals need not erect towering walls or refuse to leave their homes to shield themselves from pervasive government surveillance. Instead, Mora and Suarez's attestation that they neither consented to, nor expected that, their private property would be subject to ongoing surveillance is enough to establish a subjective expectation of privacy. What is more, this expectation is objectively reasonable. Just like the government's use of GPS or CSLI technology to track an individual's location, the Commonwealth's prolonged pole camera surveillance of Mora and Suarez's homes allowed law enforcement to shed the constraints of physical surveillance and collect intimate details about their lives that were otherwise unknowable. Such actions require a warrant even where the information is publicly exposed. (pp. 23-31).

3. Applying the warrant requirement in this case is especially necessary for two reasons. First, affirming the Superior Court's opinion would expose people to increasingly advanced technology that will enhance the Commonwealth's surveillance capabilities even further. This includes already-available technology that, if applied to home-trained pole cameras, could allow officers to zoom, search and use the footage in increasingly invasive ways. This Court's ruling here must take account of these more sophisticated systems. Second, refusing to apply the warrant requirement to long-term pole camera surveillance of homes would

particularly harm individuals without the financial means to replace constitutional privacy protections with those protections—such as large plots of land and expensive physical barriers—that must be purchased. Art. 14 and Fourth Amendment protections are not, and should not become, a luxury. (pp. 31-37).

## ARGUMENT

### I. The Commonwealth's use of electronic surveillance to collect information that it could not obtain through traditional surveillance constitutes a search that triggers the warrant requirement of art. 14 and the Fourth Amendment.

"Under both the Federal and Massachusetts Constitutions, a search in the constitutional sense occurs when the government's conduct intrudes on a person's reasonable expectation of privacy." *Augustine*, 467 Mass. at 241.Where an individual has a reasonable expectation of privacy, a search is "per se unreasonable" unless conducted pursuant to a judicial warrant. *Arizona v. Gant*, 556 U.S. 332, 338 (2009). Here, the Commonwealth surveilled homes with continuous video monitoring for periods of up to five and a half months. Although the cameras observed activities visible from the street, both the U.S. Supreme Court and this Court have held that a reasonable expectation of privacy may encompass such actions. See, e.g., *Carpenter*,138 S. Ct. at 2217 (government's acquisition of long-term CSLI violated a reasonable expectation of privacy protected by the Fourth Amendment, even though CSLI records information about location and movements that could be observed by members of the public);

*Augustine*, 467 Mass. at 247-255 (same under art. 14); *Rousseau*, 465 Mass. at 378-382 (government's acquisition of long-term GPS information violated a reasonable expectation of privacy protected by art. 14, even though GPS information reveals location and movements in public).

These cases set forth two principles to guide this Court's analyses of whether someone has a reasonable expectation of privacy in activities that have arguably been exposed to the public. First, people do not need to take extraordinary measures to manifest a subjective expectation of privacy from electronic intrusion. And second, individuals retain an objectively reasonable expectation of privacy in information that practically could not be obtained via traditional surveillance.

### A. Art. 14 and the Fourth Amendment do not require people to take extraordinary measures to preserve a subjective privacy interest against pervasive technological intrusion.

Individuals can establish subjective privacy interests in information about themselves even if they do not take heroic measures to thwart government access to that information. For instance, the Supreme Court has rejected the suggestion that people should be required to add extra insulation to their homes to avoid police surveillance using thermal-imaging equipment, compare *Kyllo*, 533 U.S. at 29–40, with *id*. at 45 (Stevens, J., dissenting), and has made clear that people need not "disconnect [their] phone from the network" to prevent police from searching their location data, *Carpenter*, 138 S. Ct. at 2220. Similarly, this Court has found

that individuals demonstrate a subjective expectation of privacy in their phones' location simply by virtue of the fact that they obtained their phone for personal use, not to share information with the government. See *Almonor*, 482 Mass. at 35 n.7; *Augustine*, 467 Mass. at 255 & n.38; see also *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) (defendant "plainly manifested" a subjective expectation of privacy in emails that were fully accessible to his email provider "[g]iven the often sensitive" contents of the communications). As these cases demonstrate, neither art. 14 nor the Fourth Amendment requires a person to alter their normal daily life to protect themselves from government intrusion.

### B. Art. 14 and the Fourth Amendment recognize an objectively reasonable expectation of privacy in detailed information gathered through technology that is effectively unknowable via traditional surveillance.

To preserve "that degree of privacy against government that existed when the Fourth Amendment and art. 14 were adopted," *Almonor*, 482 Mass. at 54 (Lenk, J. concurring) (cleaned up), courts have held that the government's use of technology to collect "detailed, encyclopedic, and effortlessly compiled" information that is "otherwise unknowable" via traditional techniques, triggers a warrant requirement, *Carpenter*, 138 S. Ct. at 2216, 2218; see also *Almonor*, 482 Mass. at 46. This constitutional protection covers information that is either impossible or impracticable to collect via physical surveillance.

Before the digital age, "the greatest protections of privacy were neither constitutional nor statutory, but practical," as physical surveillance of any significant duration was so "difficult and costly" it was "rarely undertaken." *United States v. Jones*, 565 U.S. 400, 429 (2012) (Alito, J. concurring). Technology has rendered such monitoring "relatively easy and cheap," destroying the checks and balances that previously limited the government's ability to surveil its citizens. *Id*. This Court has recognized that the Commonwealth "may use electronic devices to monitor an individual's movements in public to the extent the same result could be achieved through visual surveillance." *Augustine*, 467 Mass. at 252. In so doing, however, it has made clear that individuals retain a reasonable expectation of privacy in information that was *theoretically* possible, but *practically* unlikely, for the government to collect via physical surveillance due to logistical hurdles. See, e.g., *Commonwealth v. Norman,* Sup. Jud. Ct., No. 12744, slip op. at 7 (Mar. 17, 2020); *Almonor*, 482 Mass. at 46; *Rousseau*, 465 Mass. at 381; see also *Commonwealth v. Connolly*, 454 Mass. 808, 833-835 (2009) (Gants, J. concurring); *Jones*, 565 U.S. at 415-16 (Sotamayor, J. concurring); *id.* at 429-430 (Alito, J. concurring).

For example, this Court held that the Commonwealth's use of electronic surveillance for extended location tracking triggers the warrant requirement. *Rousseau*, 465 Mass. at 382. Historically, officers could obtain this information

"through physical surveillance conducted seven days per week, twenty-four hours per day." *Connolly*, 454 Mass. at 833 (Gants, J. concurring). Such monitoring, however, was resource-intensive and subject to community detection and hostility. *Rousseau*, 465 Mass. at 381; *Jones*, 565 U.S. at 415-416 (Sotomayor, J. concurring). As a result, "society's expectation has been that law enforcement agents and other would not —and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Jones*, 565 U.S. at 430 (Alito, J. concurring) (quoted in *Augustine*, 467 Mass. at 247 n.32). Because GPS enables law enforcement to evade these "ordinary checks" on location tracking, this Court held that "a person may reasonably expect not to be subjected to extended GPS electronic surveillance by the government, targeted at his movements" without a warrant. *Rousseau*, 465 Mass. at 382; see also *Norman,* slip op. at 7 (holding pre-trial individuals have a reasonable expectation of privacy against GPS monitoring because "GPS monitoring continuously tracks an individual's precise location, thereby giving probation officer and police access to a category of information otherwise unknowable") (cleaned up); *Almonor*, 482 Mass. at 46 (noting officers could "patrol streets, stake out homes, interview individuals, or knock on doors to locate persons of interest," before holding individuals can reasonably expect the

government not to use cellular GPS to more efficiently locate their real time location).

Under this case law, an individual's reasonable expectation of privacy is implicated when the Commonwealth uses technological surveillance to collect the range of familial, personal, political, medical and religious information that "'provide[s] an intimate picture of one's daily life'" which is essentially, if not entirely, unobtainable via physical surveillance. *Augustine*, 467 Mass. at 248 (quoting *New Jersey v. Earls*, 214 N.J. 564, 586 (2013)); see also *Jones,* 565 U.S. at 416 (Sotomayor, J. concurring) (noting "I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques" where the latter was subject to "limited police resources and community hostility").

## II. Training a pole camera on a home for long-term, continuous surveillance violates constitutionally protected privacy interests.

The principles and case law described above cut strongly in favor of requiring the Commonwealth to get a warrant where, as here, it trains a pole camera at someone's home over an extended period. It is difficult to imagine a situation in which a person would lack a subjective expectation that they can live their life free from continuous, prolonged recording of every event occurring immediately outside of their home. This expectation is reasonable because, as with CSLI and GPS, home-facing cameras create a "detailed, encyclopedic, []

effortlessly compiled" and "deeply revealing" catalog of information that is practically unobtainable via traditional surveillance methods. *Carpenter*, 138 S. Ct. at 2216, 2223.

### A. Surreptitious pole camera surveillance of a home violates an individual's subjective expectation of privacy.

Mora and Suarez have both attested that they did not consent to any search of their property and they did not expect their private property to be subject to ongoing government surveillance. App. 40, 58. Under this Court's jurisprudence, those attestations are sufficient to establish subjective expectations of privacy against home-trained pole camera surveillance. Cf. *Augustine*, 467 Mass. at 255 & n.38 (holding "defendant made a showing of a subjective privacy interest" in his cell site location information where he "submitted an affidavit stating that he acquired his cellular phone for his own personal use" and "never permit[ed] the police or other law enforcement officials access to his telephone records"). And for good reason. If a typical person were to turn on the television only to find that it is showing five and a half consecutive months of footage that some stranger took of the front of their home, they would not likely think this was merely the price of having a house that is visible from the street.

In the Superior Court, the Commonwealth argued otherwise. It claimed that, when a person does not erect a fence, wall, or otherwise obstruct the street view of the front of their home, it denotes a lack of a subjective expectation of privacy

against the continuous, prolonged recording of all events that occur around their front door. See App. 74. But that is not the law. If a person need not abandon their use of a cell phone to avoid government surveillance of their historic location data, cf. *Carpenter*, 138 S. Ct. at 2220, people surely need not build a wall or refrain from leaving their home or from inviting guests to the same to avoid exposing their familial, political, professional, religious, and sexual associations to government surveillance. Accepting the Commonwealth's position would require people to erect towering walls around their homes to shield themselves from pervasive video surveillance; art. 14 and the Fourth Amendment do not require such a radical, and expensive, step to retain constitutional protections. See also *infra* Section III(B).[5]

### B. Prolonged pole camera surveillance of a home significantly encroaches upon traditional spheres of privacy otherwise unknowable via traditional surveillance.

Although the prolonged pole camera surveillance of the homes of Mora and Suarez presents an issue of first impression in this Court, the Court's prior decisions indicate that this technique implicated objectively reasonable

[5] Standard utility poles for residential power delivery are approximately 40 feet tall. See David Brooks, *There are 500,000 Utility Poles in New Hampshire, Yet We Hardly Notice Them*, Concord Monitor (Dec. 24, 2016), https://perma.cc/XT7U-8MYT. Erecting a wall high enough to block a camera mounted on a pole would be difficult and cost prohibitive for all but a very few.

expectations of privacy because it enabled law enforcement to shed traditional surveillance constraints and reveal intimate details about Mora and Suarez's lives.[6]

First, just like longer-term location monitoring via GPS or CSLI, such monitoring would have been effectively impossible via physical surveillance. Here, the cameras provided round-the-clock, continuous surveillance of the front of Mora and Suarez's homes for 168 and 61 days—or 4,032 and 1,464 hours—respectively. A police stakeout on a residential street would not evade detection for a few days, let alone months at a time.[7] Even if it could, at the lowest MSP pay scale in 2017, this months-long stakeout would have cost more than $40,000.[8] In comparison, the pole camera surveillance was "remarkably easy, cheap, and efficient," enabling the monitoring "at practically no expense." *Carpenter*, 138 S. Ct. at 2218. And, like

---

[6] The Commonwealth's lengthy string cite to cases evaluating pole camera surveillance does not suggest otherwise. See App. 80-82. None of the cases stem from this Court and the vast majority were issued prior to the 2018 *Carpenter* decision. The remaining cases consist of three unpublished decisions from federal courts in Wisconsin, a single unpublished decision from a federal court in Illinois, and a single decision addressing the inapposite video surveillance of a commercial business. App. 81-82.

[7] Cf. *United States v. Vargas*, No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672, at *26 (E.D. Wash. Dec. 15, 2014) ("[I]t may have been possible for law enforcement agents to take turns personally observing [defendant's] activities in his front yard for a thirty-day period but the success of such hypothetical constables going unnoticed by [the defendant] for thirty days is highly unlikely.").

[8] In 2017, the lowest MSP salary was $2,521.69 on a bi-weekly basis. See Mass.gov, Guide: Salary Compensation, https://perma.cc/AC8B-NHAJ. Alternatively, the highest MSP salary was $5,065.99 every two weeks. *Id.* At that rate, the cost of a single officer monitoring the homes of Mora and Suarez would have exceeded $80,000.

utilizing GPS or CSLI, placing a camera atop a pole allowed the officers to conduct such surveillance without detection. Cf. *United States v. Karo*, 468 U.S. 705, 709 (1984) (noting police used technology to monitor a car's location where "the agents did not maintain tight surveillance for fear of detection"). In this way, as the Commonwealth itself noted below, the cameras could "conduct surveillance for a longer period of time at lower cost and with less likelihood of detection" than an officer. App. 83.[9]

Second, the pole cameras trained on a Mora and Suarez's homes enabled the officers to chart out a detailed picture of their private lives. The cameras recorded the patterns and timing of their movements to and from home, the items they carried with them when they left and arrived, and the people who visited them and how long those visitors stayed. It matters not that some degree of inference may have been required to fill in the blanks; the Supreme Court has "rejected the proposition that 'inference insulates a search.'" *Carpenter*, 138 S. Ct. at 2218

[9] Notably, while law enforcement may have been able to watch limited durations of live or recorded footage from traditional surveillance cameras in the past, their current ability to remotely manipulate these cameras, view their footage in real-time via web-based browser, and inexpensively store and digitally analyze massive amounts of data indefinitely, has radically altered their capabilities. See, e.g., Jay Stanley, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy, American Civil Liberties Union* (2019), https://perma.cc/P3N8-TUKZ (contrasting "a surveillance camera in a typical convenience store in the 1980s," which was "big and expensive, and connected by a wire running through the wall to a VCR sitting in a back room," with "[t]oday's capture-and-store video systems [that] are starting to be augmented with active monitoring technology").

(quoting *Kyllo*, 533 U.S. at 36). Collecting such information for months at a time was amply revealing to impinge upon the "privacies of life." *Id*. at 2217.

The Commonwealth argued below that Mora and Suarez did not retain a reasonable expectation of privacy in this information because it was "exposed to the public," App. 75, and "neither [the] federal nor [the] Massachusetts constitution punishes law enforcement for using technology to more efficiently investigate crime," App. 77-78. But as described above, both the Supreme Court's and this Court's decisions regarding lengthy location tracking via GPS or CSLI stand for the exact opposite proposition. Where, as here, the Commonwealth uses technology to obtain information that it was effectively unable to collect via physical surveillance due to resource constraints, that action triggers a warrant requirement even where the information was publicly exposed. See e.g., *Rousseau*, 465 Mass. at 379-382; *Carpenter,* 138 S. Ct. at 2216-2224.

The Commonwealth's remaining argument, adopted by the Superior Court, is that the logic behind the CSLI and GPS cases is limited to location tracking and does not apply to the deployment of "stationary" cameras, even when they are trained on homes. App. 79-80, 120, 122. This argument misses the central point of the CSLI and GPS cases, which recognized protections for location information not because location information alone is special, but because location information implicitly reveals *other* private information about a person's life. As *Carpenter*

explained, lengthy location tracking "provides an intimate window into a person's life, revealing not only his particular movements, but *through them* his 'familial, political, professional, religious, and sexual associations.'" 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring)) (emphasis added); see also *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that *reflects* a wealth of detail about her familiar, political, professional, religious, and sexual associations.") (emphasis added). Indeed, the very reason this Court found Justice Sotomayor's statements about GPS monitoring to "have particular resonance in relation to the government's acquisition of CSLI" was because both technologies "'make[] available at a relatively low cost such a substantial quantum of intimate information'" that could "reveal private aspects of identity.'" *Augustine,* 467 Mass. at 248 n.33 (quoting *Jones,* 565 U.S. at 416 (Sotomayor, J. concurring)).

These concerns apply with at least the same force to lengthy pole camera monitoring of a home. It is true that such surveillance "does not follow its subjects into private residences, doctor's offices, hospitals, political headquarters, houses of worship" and "locations of sexual liaisons." App. 123. Because its fixed location is the home itself, however, the surveillance reveals similarly intimate information. Watching a resident leave home on Sunday morning with a hymnal, Saturday

morning with a prayer shawl, or mid-day Friday with a prayer rug reveals details of religious observance. Leaving with a protest sign or an oversized X-ray film envelope suggests political activity or medical travails. A visitor arriving at the house on a weekend evening with flowers could reveal a romantic liaison, while that visitor spending the night when the homeowner's spouse is away might disclose an affair.

In other words, while the *manner* in which home-trained pole camera surveillance reveals such intimate details is different than for GPS or CSLI location tracking, the *depth and substance* of the revelation is much the same. This Court has "long looked to whether an intrusion implicates a constitutionally protected area, such as the home" when "evaluating reasonable expectations of privacy in new contexts." *Almonor*, 482 Mass. at 60 (Lenk, J. concurring); see also *Augustine*, 467 Mass. at 252 (noting special protection against government surveillance "when the monitoring involves a person's home because of the person's fundamental privacy interest attached to that location"). As a result, it would be passing strange for such intimate details to retain constitutional protections when they are collected from public streets but not when they are collected from directly outside the home.[10] To avoid this incongruous result, this

[10] Constitutional protection for the home includes the curtilage, or the area immediately surrounding it, to protect the "intimate activity associated with the sanctity of a man's home and the privacies of life." *Oliver v. United States,* 466

Court should hold that long-term pole camera surveillance of a home triggers the warrant requirement and should grant the motion to suppress.[11]

## III. Declining to provide constitutional protections against lengthy pole camera surveillance of a home would have significant long-term consequences.

Affirming the Superior Court's opinion would leave the people of the Commonwealth at the mercy of increasingly advanced technology. The weight of such a decision would also impact those who are already most vulnerable due to their lack of resources to guard against government surveillance at a time when the economic disparity gap is only increasing.

### A. A warrant requirement is particularly necessary because law enforcement in Massachusetts already use technologies that could enhance the surveillance capabilities of pole cameras even beyond what occurred in this case.

In assessing whether the Commonwealth's use of home-trained pole cameras

---

U.S. 170, 180 (1984) (cleaned up); see also *Commonwealth v. Leslie*, 477 Mass. 48, 56-58 (2017) (defendant's porch and side yard were part of the home's curtilage); *Commonwealth v. Fernandez*, 458 Mass. 137, 143-147 (2010) (a narrow driveway adjacent to a triplex was within an apartment's curtilage).

[11] The Commonwealth separately argues that exclusion should not apply here "[b]ecause there is no indication of any misconduct and the police acted in good faith," App. 87, but this Court does "not recognize a 'good faith' exception" to the exclusionary rule. *Commonwealth v. Fredericq*, 482 Mass. 70, 84 (2019). While this Court has recognized that the exclusionary rule need not apply where the violations are not "substantial and prejudicial," *Commonwealth v. Hernandez*, 456 Mass. 528, 533 (2010), the collection of thousands of hours of video surveillance from Mora and Suarez's homes that formed the basis for several warrant applications is anything but insubstantial or non-prejudicial.

threatens to "shrink the realm of guaranteed privacy," this Court must consider not only the technology used here, but also related, existing technologies that could further enhance surveillance capabilities. *Kyllo*, 533 U.S. at 34; see also *Almonor*, 482 Mass. at 44, 47 n.13; *Connolly*, 454 Mass. at 835. "[T]he 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 (cleaned up). Here, technology is developing in at least three ways that warrant consideration in this case.

First, video cameras can now hone in on small details with startling accuracy that goes well beyond the capabilities of the human eye. One company has released a camera small enough to be affixed to a drone, which can identify a face from 1,000 feet and read serial numbers from 100 feet.[12] Canadian casinos have used cameras to zoom in and read text messages off a phone.[13] And nearly ten years ago, Logan Airport installed a camera that could see any object a centimeter-and-a-half wide from 150 meters.[14] That is a distance of more than one-and-a-half football fields. According to the MassPort director of corporate security, "the next version is going to be twice as powerful."[15] Deployed on a home-facing camera,

---

[12] Jason Koebler, *This Drone Zoom Lens Can Identify Your Face from 1000 Feet Away*, VICE (Feb. 25, 2015), https://perma.cc/GVM7-L5B2.
[13] Lori Culbert, *Judge Raps Police for Using Casino Cameras to Read Suspect's Texts*, Vancouver Sun (Nov. 11, 2014), https://perma.cc/T3EE-ZC7T.
[14] Brian R. Ballou, *At Logan, New Device Keeps Eye on Everything*, Boston Globe (May 3, 2010), https://perma.cc/YYP3-ENMD.
[15] *Id.*

these zoom-capabilities could enable officers to read anything coming into or out of a surveilled house, such as credit card statements, immigration papers, texts from a spouse or child, or passwords.

Second, existing technology enables the rapid "search of volumes of video that would otherwise be impossible."[16] Software like "BriefCam" allows officers to quickly review hours of video by simultaneously displaying events that occurred at different times.[17] BriefCam also classifies the properties of images, allowing officers to use keywords to search images in 27 categories including gender, age, and "appearance similarity."[18] Applied to home-facing cameras, such technology could further decrease the resources necessary to surveil an individual's house for months on end.

Third, many law enforcement officers warrantlessly utilize face surveillance technology, which threatens to amplify the intrusion of their use of warrantless home-facing cameras.[19] Officers can now run an image—such as a still taken from

---

[16] BriefCam, *Video Analytics Solutions for Post-Event Investigations,* https://perma.cc/9T3K-K3TN; see also Stanley, *The Dawn of Robot Surveillance*, *supra* note 9.
[17] BriefCam, *Technology That Allows You to Review Video Fast,* https://perma.cc/75WW-CMZ7.
[18] BriefCam, *Intelligent Video Analytics Solutions,* https://perma.cc/9MDZ-MBRU; BriefCam, *Search & Review Hours of Video in Minutes: Solutions to Help Investigators Accelerate Investigations*, https://perma.cc/6ZJJ-2QLW.
[19] Face surveillance technology "is the automated process of comparing two images of faces to determine whether they represent the same individual." Clare Garvie, Alvaro Bedoya and Jonathon Frankle, *The Perpetual Line-Up:*

video footage—against a database of photographs—such as drivers' licenses or booking photographs—to identify an individual. In 2015, federal, state and local law enforcement agencies made 258 requests to the Massachusetts Registry of Motor Vehicles (RMV) asking the agency to compare images against the RMV's database to identify an individual, "the equivalent of about one request per weekday."[20] Local police departments are also among the "376 law enforcement agencies [that] have access to a database of 2.6 million photos of people who are arrested and booked" in the Commonwealth.[21] Applying this technology to still images taken from a home-trained camera, police could identify everyone entering or exiting that house.

### B. Authorizing warrantless, prolonged pole camera surveillance of a home would disparately impact those with the fewest resources to protect themselves from surveillance.

Although affirming the Superior Court's order would threaten everyone's reasonable expectation of privacy in their homes, it would have an especially negative impact on people with limited financial means who cannot replace constitutional privacy protections with expensive properties and enhanced

---

*Unregulated Police Face Recognition in America*, Center on Privacy and Technology (Oct 18, 2016) https://perma.cc/WNP3-6LBR; see also Stanley, *The Dawn of Robot Surveillance*, *supra* note 9.

[20] Jim Davis, *State Scans Mass. License Photos to Find Matches with Suspects*, Boston Globe (Dec. 20, 2016), https://perma.cc/7DLH-T4QD.

[21] *Id.*

technology. The Supreme Court has long emphasized, "the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion." *Karo*, 468 U.S. at 731 (citing *United States v. Ross*, 456 U.S. 798, 822 (1982)). But without the Constitution, the best defense against warrantless pole camera surveillance might be something that only money can buy: having a large property with a dwelling that is set back from public streets and sidewalks. A decision that does not recognize constitutional protections against warrantless pole camera surveillance therefore may tend to "apportion [article 14 and] Fourth Amendment protections on grounds that correlate with income, race, and ethnicity." *Commonwealth v. Leslie*, 477 Mass. 48, 54 (2017) (cleaned up).

The gulf between those who have expendable resources and those who do not is growing. According to data from the U.S. Census Bureau, "the gap between the richest and the poorest U.S. households is now the largest it's been in the past 50 years."[22] In Massachusetts, the contrast is even more striking. In 2015, Massachusetts had the sixth highest income inequality in America; the next year, Boston had the seventh highest income inequality among American cities.[23]

---

[22] Bill Chappell, *US Income Inequality Worsens, Widening to a New Gap*, NPR (Sept 26, 2019), https://perma.cc/6XHD-4FR6; see also United States Census Bureau, Press Release: American Community Survey Provides New State and Local Income, Poverty and Health Insurance Statistics (Sept. 26, 2019), https://perma.cc/RE62-23MN.

[23] Luc Schuster & Peter Ciurczak, *Boston's Booming . . . But for Whom?,* Boston Indicators and the Boston Foundation, at 16 (Oct. 2018), https://perma.cc/5KZT-HECU.

What's more, these numbers contain troubling racial disparities. White household income in Boston was approximately double that of any other racial group in 2016.[24] "[E]ven greater than [these] gaps in income," however, is the "large, persistent racial wealth gap."[25] The median family wealth of white families living in the metro Boston area in 2015 was $247,500; it was $3,020 for a Puerto Rican family, $8 for a Black family, and $0 for a Dominican family.[26]

When it comes to avoiding pole camera surveillance of the home, wealth matters. For example, wealthy people can purchase homes in gated communities or neighborhoods with underground utility poles, where it is more difficult for police to affix a camera. They can buy expansive plots of land with houses set so far back that they obscure any camera angle. They can even build underground tunnels for entry or enclose their entire home with tinted glass to prevent a camera from seeing their front door.[27] In other words, if the Constitution is deemed not to afford them a protected space, they can afford to buy one.

People of lesser means will not be so lucky. Without the ability to afford such neighborhoods, houses, or technology, those with less will be more subject to

---

[24] *Id.* at 21.
[25] *Id.* at 34.
[26] *Id.*
[27] Such measures are neither impossible nor improbable for those with resources. For example, to combat drone surveillance, one company trained eagles to bring down the devices. See Jon Hegranes, *The Past, Present and Future of Anti-Drone Tech*, Forbes: Council Post (Jan 26, 2018, 7:30 AM), https://perma.cc/9479-S8F8.

the warrantless surveillance of their most private movements. Under art. 14 and the Fourth Amendment, privacy should not be cost-prohibitive for some while available to others.

## CONCLUSION

For the foregoing reasons, this Court should reverse the Superior Court. Of course, the implication of such a ruling is not that law enforcement will never be able to engage in the kind of surveillance at issue in this case; rather, the "answer to the question of what police must do before [conducting extended pole camera surveillance of a home] is accordingly simple—get a warrant." *Riley v. California*, 573 U.S. 373, 403 (2014).

Date: March 20, 2020

Respectfully submitted,

*/s/ Matthew R. Segal*

Matthew R. Segal (BBO 670685)
Jessie J. Rossman (BBO 654489)
Kristin M. Mulvey (BBO 705688)
American Civil Liberties Union Foundation of Massachusetts, Inc.
211 Congress Street
Boston, MA 02110
617.482.3170
msegal@aclum.org
jrossman@aclum.org
kmulvey@aclum.org

Nathan Freed Wessler (BBO 680281)
Brett Max Kaufman (on the brief)
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
212.549.2500
nwessler@aclu.org
bkaufman@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
andrew@eff.org

Gregory T. Nojeim (DC 398337)
Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, DC 20005
202.637-9800
gnojeim@cdt.org

*Counsel for Amici*

## CERTIFICATE OF COMPLIANCE

I, Jessie J. Rossman, do hereby certify that this brief complies with the rules of court that pertain to the filing of amicus briefs, including, but not limited to Rule 16, 17 and 20. This brief complies with the length limit because it is set in 14-point Times New Roman font, and contains 6,859 non-excluded words, as determined through use of the "word count" feature in Microsoft Word 2010.

*/s/ Jessie J. Rossman*
Jessie J. Rossman

## CERTIFICATE OF SERVICE

I, Jessie J. Rossman, do hereby certify that on March 20, 2020, I served this brief on the Commonwealth and the defendants by directing an electronic copy of the foregoing brief to the following counsel:

Stephen D. Judge
Hemsey Judge, PC
47 Federal Street
Salem, MA 01970
sjudge@hemseyjudge.com

Mark G. Miliotis
Prince Building
63 Atlantic Avenue
Boston, MA 02110
Milo12@aol.com

Elliot Weinstein
83 Atlantic Avenue
Boston, MA 02110
elliot@eweintsteinlaw.com

Gina Masotta
Anna Lumelsky
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
Gina.masotta@state.ma.us
Anna.lumelsky@mass.gov

*/s/ Jessie J. Rossman*
Jessie J. Rossman

No. SJC-12890

---

COMMONWEALTH,
RESPONDENT-APPELLEE,

v.

Nelson Mora & others
PETITIONERS-APPELLANTS.

---

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., THE ELECTRONIC FRONTIER FOUNDATION, AND THE CENTER FOR DEMOCRACY AND TECHNOLOGY

---