Commonwealth of Massachusetts
Supreme Judicial Court

SJC-13816

COMMONWEALTH OF MASSACHUSETTS,
Plaintiff-Appellee,
v.

JOSE ARIAS,
Defendant-Appellant.

ON APPEAL FROM A JUDGMENT OF THE SUFFOLK SUPERIOR COURT

BRIEF OF *AMICI CURIAE* MAILYN FIDLER AND THE ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF APPELLANT AND REVERSAL

November 12, 2025

Mason A. Kortz (BBO #691257)
HARVARD LAW CYBERLAW CLINIC
1557 Massachusetts Avenue, 4th Floor
Cambridge, MA 02138
(617) 495-2845
mkortz@law.harvard.edu

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21, the Electronic Privacy Information Center represents that it is a non-profit corporation with no parent corporation or issued stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

STATEMENT OF INTEREST[1]

Professor Mailyn Fidler is a Visiting Assistant Professor at Harvard Law School, on leave from the University of New Hampshire Franklin Pierce School of Law. She teaches and writes at the intersection of criminal law, criminal procedure, and technology. Her work has been drawn on by, among other places, the U.S. Department of Justice, the District Court for the Western District of Kentucky, and the multilateral Pall Mall Process on Cyber Intrusion Capabilities. Prior to joining legal academia, Fidler clerked on the Tenth Circuit Court of Appeals and served as the Tech & First Amendment Fellow at the Reporters Committee for Freedom of the Press.

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely participates as *amicus curiae* in federal and state courts in cases concerning privacy and civil liberties. EPIC has an interest in upholding Fourth Amendment protections

[1] Pursuant to Mass. R. App. P. 17(c)(5), *amici* and their counsel declare that: (a) no party or party's counsel authored the brief in whole or in part; (b) no party or party's counsel contributed money that was intended to fund the preparation or submission of the brief; (c) no person or entity—other than *amici* or their counsel—contributed money that was intended to fund the preparation or submission of the brief; and (d) neither *amici* nor their counsel represent or have represented any of the parties to the present appeal in another proceeding involving similar issues, or were a party or represented a party in a proceeding or legal transaction that is at issue in the present appeal.

against unreasonable searches and seizures. In particular, EPIC is focused on fighting the erosion of constitutional privacy rights due to the emergence of new technologies. *See, e.g.*, *Rodriguez v. Mass. Parole Bd.*, 490 Mass. 596 (2022); *Attorney General v. Facebook*, 487 Mass. 109 (2021). EPIC has warned about the risk of mass surveillance with use of technologies such as license plate readers.

ARGUMENT

A twenty-four-hour delay in conducting a traffic stop is unreasonable. As Appellant argues, a significant delay in enforcement undermines any government interest justifying a traffic stop. As warrantless seizures based on civil infractions, traffic stops are exceptional; their legitimacy is premised on the government's need to quickly respond to potential hazards on public roads. After twenty-four hours, such an interest has long since dissipated. To the extent delayed enforcement deters future hazards, Massachusetts law provides for citations to be delivered by mail, obviating the need for an after-the-fact traffic stop. As such, *amici* endorse Appellant's argument on the motion to suppress.

Amici submit this brief to emphasize a separate point: substantially delayed traffic enforcement, combined with modern surveillance technology, increases the risk of unlawful, pretextual traffic stops in two ways. First, because modern traffic surveillance is constant and pervasive, more potential traffic violations are available for police review. Under the Commonwealth's view of the law, police are free to choose which traffic violations warrant an in-person stop and which should be handled by a mailed citation. This Court's own findings on police use of discretion suggest that officers might make this choice based on unrelated, protected characteristics like race. Second, and perhaps even more concerning, the Commonwealth's position would allow police to conduct traffic stops without an

articulable, reasonable suspicion of criminal activity. If they want to question a person of interest, police could simply search surveillance records for a civil traffic infraction documented in the last twenty-four hours—or set up an alert for when such an infraction occurs—and use that as the basis to conduct a stop that would be otherwise impermissible. Such bootstrapping would be akin to an unconstitutional general warrant. To head off such abuses of power, *amici* respectfully urge the Court to reverse the lower court decision and hold that the traffic stop in this case was unreasonably delayed and, therefore, unconstitutional.

I. A TWENTY-FOUR-HOUR DELAY IN ENFORCING A TRAFFIC STOP IS UNREASONABLE BECAUSE NO LEGITIMATE GOVERNMENT INTEREST IS BEING MET.

A traffic stop, like any seizure, is reasonable only so long as there is an "objective legal justification" for it. *Commonwealth v. Buckley*, 478 Mass. 861, 865 (2018). One such justification is the observance of a traffic violation by a law enforcement officer. *See id*. at 866. This justification is rooted in "'[the] significant government interest' of ensuring public safety on our roadways." *Commonwealth v. Daveiga*, 489 Mass. 342, 350 (2022) (quoting *Buckley*, 478 Mass. at 869). By the same token, when this interest disappears, a traffic stop is no longer reasonable. *See id*. at 351. Here, there was no safety concern because the traffic infraction occurred twenty-four hours before the stop. The stop was also unnecessary for deterring future

driving infractions because the legislature has established different procedures for issuing citations after an infraction has occurred.

First, the stop was unnecessary in ensuring safety as the stop occurred more than twenty-four hours later. As this Court explained in *Commonwealth v. Daveiga*, "[i]f objective circumstances exist showing that the government's interest in ensuring traffic safety has ended . . . , police authority to conduct a traffic stop must terminate." 489 Mass. at 351. One circumstance that marks the end of the government's interest in ensuring traffic safety is "when an officer observes a traffic violation but unreasonably delays initiating a traffic stop on the basis of that violation." *Id*. As Appellant correctly points out, where a day has passed and a motorist has been off the road for a significant time, the likelihood that any ongoing safety issue exists is minimal. *See* Appellant's Brief at 22.

Outside of immediate safety, the government's only interest in punishing past traffic violations is to deter future ones. However, this does not require an in-person stop. The Massachusetts legislature has already established a reasonable alternative procedure for enforcement when a stop at the time and place of the infraction is impossible: "the citation shall be delivered to the violator or mailed to him at his . . . address." Mass. Gen. Laws c. 90C, §2. The law expressly states that after-the-fact citations must be justified by practical reasons, including "where the violator could not have been stopped" at the time of the violation. *Id*. The existence of this option

suggests that the legislature considered the possibility that a contemporaneous stop would be impossible and gave police the power to issue citations by mail—but not the power to initiate in-person stops twenty-four hours later. This gives police appropriate enforcement power while ensuring that traffic stops bear some temporal nexus to the observation of an infraction. Police cannot ignore this option and instead opt to perform a stop after a significant delay simply because they prefer the investigative possibilities of an in-person interaction.

II. ELECTRONIC SURVEILLANCE IS PERVASIVE AND EXPANDS POLICE DETECTION OF TRAFFIC VIOLATIONS.

Law enforcement agencies utilize a wide array of digital tools—surveillance cameras, license plate readers, and facial recognition systems, to name a few—to track human behavior. This information can then be fed into data-driven predictive policing tools, allowing law enforcement to build a comprehensive picture of an individual's past movements and rapidly (albeit not always accurately) predict their future ones. The outcome is pervasive surveillance: always on, widespread, and hungry for people's data. Pervasive surveillance has affected nearly every aspect of policing, and traffic enforcement is no exception.

A. Expansive, "always-on" surveillance networks constantly capture and analyze individuals' movements and behaviors.

Technological advancements and private-public partnerships have transformed traditional policing tools into systems of "always-on" surveillance. A

common example is automated license plate readers ("ALPRs"), systems that use high-speed cameras to capture license plates and record the date, time, and location of passing vehicles. *See* Electronic Frontier Foundation, *Automated License Plate Readers* (Oct. 1, 2023).[2] Armed with a license plate number, police can query an ALPR's associated database to see where a vehicle has been in the past day, week, month, or even year. ALPR systems have been in use for decades, during which their constitutionality has been repeatedly questioned. *See, e.g.*, *Commonwealth v. McCarthy*, 484 Mass. 493 (2020); *United States v. Yang*, 958 F.3d 851 (9th Cir. 2020). Use of ALPRs has only increased over time: as of 2020, every police department serving over one million residents, and nearly ninety percent of sheriffs' offices with 500 or more sworn deputies, reported using ALPRs. *See* Kristin Finklea, Cong. Rsch. Serv., R48160, *Law Enforcement and Technology: Use of Automated License Plate Readers* (2024).

More recently, private companies have incorporated ALPRs, along with other technologies, into massive, networked traffic surveillance systems. Perhaps the most prominent company providing these services is Flock Safety, which operates in Massachusetts and across the country and boasts capturing more than 20 billion

[2] https://sls.eff.org/technologies/automated-license-plate-readers-alprs [https://perma.cc/ZXU5-55F8]

license plates per month. *See National LPR Network*, Flock Safety.[3] Flock contracts with thousands of local police departments to install cameras that record not only a car's license plate, but also passengers and unique "vehicle fingerprints," such as the make, model, color, and other distinguishing features of the car. *Id*. Law enforcement can use Flock's tools to search for vehicles, set alerts, and share data with other agencies. *Id*.

However, Flock's services go far beyond license plate detection. "Flock Nova" touts the ability to integrate data from various sources within and, with the press of a button, between law enforcement agencies. *See Flock Nova™: Smarter Investigations, Faster Case Resolutions*, Flock Safety (Feb. 13, 2025).[4] Flock's "FreeForm" artificial intelligence ("AI") tool allows officers to search through this vast trove of data with open-ended search terms, including descriptions of individuals caught on camera. *See Flock FreeForm™*, Flock Safety.[5] Flock's "Investigations Manager" and "Multi-State Insights" products take it a step further by analyzing surveillance data to flag patterns that, according to an algorithm, suggest criminal behavior. Jay Stanley, *Surveillance Company Flock Now Using AI*

[3] https://www.flocksafety.com/products/national-lpr-network [https://perma.cc/9CXF-LKSW]
[4] https://www.flocksafety.com/blog/flock-nova-smarter-investigations-faster-case-resolutions [https://perma.cc/T5AC-WCW4]
[5] https://www.flocksafety.com/products/flock-freeform [https://perma.cc/YK4Z-A5C8]

to Report Us to Police if it Thinks Our Movement Patterns Are "Suspicious", ACLU (July 23, 2025).[6]

Flock is not the only player in the public-private surveillance industry. Axon's FususONE, which was used in Washington, D.C. during the federal takeover of the district's police, integrates data from traffic cameras, license plate readers, and other sources to create a "Real-Time Crime Center" map. Nikki Davidson, *D.C. Takeover Shows How Cities Can Lose Control of Surveillance*, Government Technology (Aug. 15, 2025).[7] Axon also offers AI tools that can generate automated alerts tailored to specific search parameters. *Axon Fusus: Artificial Intelligence*, Axon.[8] Like Flock, Axon promises to direct massive amounts of integrated data to officers, increasing their ability to surveil the public.

The surveillance networks provided by Flock and Axon extend across state lines and beyond public roadways. Current surveillance technologies come with data-sharing models that enable law enforcement agencies to access surveillance data collected across the nation. For instance, law enforcement agencies that opt to

---

[6] https://www.aclu.org/news/national-security/surveillance-company-flock-now-using-ai-to-report-us-to-police-if-it-thinks-our-movement-patterns-are-suspicious [https://perma.cc/4QR5-8LZZ]
[7] https://www.govtech.com/public-safety/d-c-takeover-shows-how-cities-can-lose-control-of-surveillance [https://perma.cc/3UW9-7HL3]
[8] https://www.axon.com/products/axon-fusus/integrated-artificial-intelligence [https://perma.cc/X756-SQKD]

share their local data with Flock's network gain the ability to search data from the network's 7,000-plus connected agencies. *See* Gideon Epstein, *Flock Gives Law Enforcement All Over the Country Access to Your Location*, ACLU of Massachusetts (Oct. 7, 2025).[9] This shared network can undermine local data retention policies: even if license plate information is deleted after a set period of time, related search records may remain accessible to use by other agencies. *See* Dug Begley, Caroline Ghisolfi & Matt deGrood, *Houston Police Use a Powerful Surveillance Tool to Track Vehicles. But They're Not Explaining Why*, Houston Chronicle (June 10, 2025).[10]

Other private companies have begun to join these surveillance networks. Ring, an Amazon-owned provider of home security products, has recently partnered with Flock and Axon to provide law enforcement agencies easier access to video feeds. *See* Omar Gallaga, *Amazon's Ring Cameras Push Deeper Into Police and Government Surveillance*, CNET (Oct. 18, 2025).[11] This partnership gives police yet another avenue to obtain surveillance data without a warrant or any form of

[9] https://data.aclum.org/2025/10/07/flock-gives-law-enforcement-all-over-the-country-access-to-your-location/ [https://perma.cc/9V6P-YRAE]
[10] https://www.houstonchronicle.com/projects/2025/houston-flock-surveillance-explained/ [https://perma.cc/5N4L-7CPC]
[11] https://www.cnet.com/home/security/amazons-ring-cameras-push-deeper-into-police-and-government-surveillance/[https://perma.cc/9ZWN-S9PW]

oversight. The end result of these partnerships is the widespread, continuous, and persistent surveillance of individuals and their movements, particularly when they are driving on public roads.

B. Modern surveillance networks give police unprecedented power that can be used in concerningly invasive ways.

The massive, networked surveillance systems being developed by Flock, Axon, and other companies greatly expand law enforcement agencies' information collection powers. Police can quickly search massive troves of data, locate individual people or vehicles, and follow them across state lines. These queries can be made forward-looking, by setting automated alerts, or backward-looking, by searching existing video records. All of this power is ripe for abuse—a concern that is far from hypothetical.

In 2024, authorities in Texas conducted a nationwide search through Flock's license plate reader database, not for a stolen vehicle or a criminal suspect, but for a woman who had a self-administered abortion. Joseph Cox & Jason Koebler, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404 Media (May 29, 2025).[12] The reason for the query was explicitly entered as "had an abortion, search for female." *Id*. The search extended across

[12] https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/ [https://perma.cc/CNN9-YHXC].

multiple states, including states where abortion is legally protected, and ultimately reached more than 83,000 cameras over the span of a month. *Id*.

Surveillance networks have also been used to single out and track groups of people based on protected characteristics. Between June 2024 and October 2025, more than eighty police departments across the United States searched the Flock system using racist or demeaning terms like "roma," "g*psy," and "roma traveler," often without citing any suspected crime. Rindala Alajaji & Dave Maass*, License Plate Surveillance Logs Reveal Racist Policing Against Romani People*, Electronic Frontier Foundation (Nov. 3, 2025)[13] One department even used Flock's "Convoy" feature to target "g*psy" vehicles traveling together. *Id*.

Traffic surveillance systems have also been exploited for illegal and invasive personal searches. In 2023, a police chief in Sedgwick, Kansas, used Flock's ALPR system 228 times over four months to stalk his ex-girlfriend and her new partner. Michael Stavola, *Kansas Police Chief Used Flock License Plate Cameras 164 Times to Track Ex-Girlfriend*, The Wichita Eagle (Aug. 17, 2024).[14] The chief entered false justifications like "drug investigation" and "suspicious activity" to disguise the

[13] https://www.eff.org/deeplinks/2025/11/license-plate-surveillance-logs-reveal-racist-policing-against-romani-people [https://perma.cc/U5AN-CJAN]
[14] https://www.kansas.com/news/politics-government/article291059560.html [https://perma.cc/97FZ-SRSJ]

searches. *Id*. The abuses were ultimately detected by a local oversight board; Flock declined any responsibility for the incident. *Id*.

Taken together, massive networks of always-on, data-driven surveillance technologies enable a form of monitoring that is continuous, borderless, and pervasive. Constant data collection and interconnected networks allow law enforcement to look forward and backward in time, across jurisdictions and even into private spaces. Such powerful surveillance tools can be—and have been—used in ways that are invasive, biased, and outright unlawful. As explained below, allowing police to bootstrap in-person traffic stops based on such surveillance data would further exacerbate this already pressing concern.

III. PERVASIVE SURVEILLANCE COMBINED WITH DELAYED, PRETEXTUAL TRAFFIC STOPS INCREASES THE RISK OF BIASED POLICING.

As this Court has recognized, "the plethora of potential traffic violations is such that most drivers are unable to avoid committing minor traffic violations on a routine basis, thereby affording officers wide discretion in the enforcement of traffic laws." *Commonwealth v. Long*, 485 Mass. 711, 718 (2020). As the facts of this case demonstrate, given enough time, police can catch almost anyone committing a traffic violation. In the Commonwealth's view, officers have the power to escalate such violations to a search and seizure, without articulable, reasonable suspicion of an underlying crime, long after the infraction was observed. *See* Appellee's Brief at 19.

As Appellant explains, it is essential that this Court takes the opportunity to address that view head on. *See* Appellant's Brief at 26–29.

While police in Massachusetts have been conducting pretextual stops for years, there has always been a natural limitation on this power: police cannot observe every car at all times on all roads with a finite number of officers. With the advent of mass traffic surveillance, however, traffic infractions everywhere may be detected and logged, far in excess of police capacity to conduct stops. If police have discretion to pick and choose which violations warrant a *post hoc* traffic stop, there is a very real risk that such choices will be biased along the same lines this Court has identified in recent cases. Moreover, modern surveillance tools allow police to identify a person of interest and actively trawl for surveillance records, including traffic violations. If such violations are held to justify later in-person stops, the police would effectively be able to conduct a seizure on anyone who was less than a perfect driver. Considering the realities of mass surveillance, it is even more imperative that the Court takes this opportunity to articulate constitutional limitations on delayed, pretextual traffic stops without reasonable suspicion.

A. If allowed to initiate delayed traffic stops without reasonable suspicion, police officers may replicate existing, biased practices.

According to the Commonwealth, a police officer who observes a traffic violation but opts not to make a stop has a choice: mail a citation, as provided for in Mass. Gen. Laws c. 90C, §2, or initiate a traffic stop at a later date. In the context of

delayed stops, this would allow police to stop, seize, and search anyone who was caught on camera breaking a traffic rule—which means almost anyone who is driving for more than a few minutes.

Unfortunately, the choice of *who* to stop is unlikely to be free of bias in all cases. If history is any indicator, police officers may make this determination based on biased perceptions of protected characteristics like race. ALPRs are already disproportionately deployed within minority communities, which can lead to further bias. *See* Shawn Musgrave, *After Public Records Request, Boston Police Suspends License Plate Scanner Surveillance Program*, MuckRock (Dec. 15, 2013) (noting greater density of ALPRs in South Boston, Roxbury, and Dorchester).[15] Moreover, the Commonwealth advances a rule that police do not need to explain their motivation for a stop, so long as a traffic violation actually occurred. *See* Appellee's Brief at 20–21. This would allow police to arbitrarily stop nearly anyone on the road, without ever having to offer an explanation.

This Court has recognized the prevalence and risk of racially motivated traffic stops and imposed limitations to prevent them. *See Long*, 485 Mass. at 715 (noting "the persistent and pernicious problem of racial profiling in traffic enforcement"); *Buckley*, 478 Mass. at 876–77 (Budd, J., concurring) ("Years of data bear out what

[15] https://www.muckrock.com/news/archives/2013/dec/15/boston-police-close-alpr-program/ [https://perma.cc/9NF6-KQ3B]

many have long known from experience: police stop drivers of color disproportionately more often than Caucasian drivers for insignificant violations (or provide no reason at all).”). In *Commonwealth v. Long*, the Court made it easier for defendants to suppress evidence arising from traffic stops motivated by race or another protected class, discouraging police from such conduct. 485 Mass. at 720. This Court has repeatedly affirmed the *Long* standard, applying it to policing conduct beyond traffic stops. *See e.g.*, *Commonwealth v. Robinson-Van Rader*, 492 Mass. 1, 3 (2023) (applying the standard to pedestrian stops), *Commonwealth v. Dilworth,* 494 Mass. 579, 586–87 (2024) (applying the standard to social media investigations).

Most recently, in *Commonwealth v. Dilworth*, the Court recognized how digital surveillance enables the same racially biased policing that is prevalent in traditional surveillance. 494 Mass. at 582. The Court held that the police were required to disclose information about its investigative practice of creating fake social media profiles using predominantly black and brown profile avatars, “friending” social media users, and then searching those users’ posts for evidence. *See id*. at 581–82. The Court held that the same standard applies to both in-person and digital investigations, disincentivizing police from importing racially biased policing methods into digital surveillance. *Id*. at 587.

Given its familiarity with how electronic surveillance amplifies biased police practices, the Court can likely anticipate how unfettered discretion to initiate traffic stops based on traffic surveillance would play out. The surveillance capabilities discussed above would not only increase the volume of information about traffic violations, but it would also increase the volume of details available about an individual driver (e.g., their skin color, what clothes they wear, who they are traveling with) and their car (e.g., the state of disrepair, what locations it frequents). *See* Jay Stanley, *Flock's Aggressive Expansions Go Far Beyond Simple Driver Surveillance*, ACLU (Aug. 18, 2025).[16] By relying on these details to determine whom to investigate, police may consciously or unconsciously base their suspicions on unrelated characteristics like race, gender, and class. As police officers are typically under no obligation to provide justifications for their searches, such improper searches will likely escape scrutiny. *See* Begley et al., *supra* p.15 (finding that, for over two-thirds of the 470,000 searches made through Flock, police officers provided a vague or meaningless explanation, including gibberish like "asdf").

Furthermore, future systems promise to outsource the determination of who to investigate to the surveillance network itself. As noted above, Flock now offers a tool to draw inferences based on the information it collects, using an algorithm to

[16] https://www.aclu.org/news/privacy-technology/flock-roundup [https://perma.cc/A3NN-PPG3].

generate "suspicion" of criminality. *See* Stanley, *supra* p.13–14. However, little is known about how these algorithms actually work. Relying on surveillance systems to determine which traffic infractions to escalate into a seizure may well reinforce existing biased policing methods in a way that is effectively unreviewable.

B. Limitless data combined with limitless discretion allows police to effectuate suspicionless stops akin to a general warrant.

The interaction between pervasive traffic surveillance and unfettered police discretion could grant new, unconstitutional powers to the police. The technological affordances of always-on surveillance are imminently relevant to a constitutional analysis. *See Carpenter v. United States*, 585 U.S. 296, 305 (2018) (noting the need to keep "Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools"). This is especially true when a new technology operates automatically against everyone at all times, storing data for undetermined retrospective use. *See id*. at 312 (noting that police access to retrospective data "runs against everyone"). Always-on, ubiquitous, automatic surveillance grants police an unprecedented power to "travel back in time" and view conduct that occurred before developing a suspicion or an interest in the subject of an investigation. *Id*. Courts have taken great care to understand and limit how that power can be used. *See* Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 HARV. L. REV. 1790, 1823 (2022)

(finding that scope and automated nature of data collection factored heavily in courts' post-*Carpenter* Fourth Amendment decisions).

Pervasive traffic surveillance raises exactly the concerns expressed in *Carpenter*. With the scale of surveillance data and the breadth of the traffic code, evidence of a past traffic infraction may be available for any given motorist. Adding a rule that allows substantial time to pass between an infraction and a stop would permit police to identify a person of interest, review surveillance records for a traffic violation, and seize them the next time that person was driving. Such power approaches that of an impermissible general warrant, allowing police to stop and search suspects with no particularity so long as they are in a vehicle and broke a traffic rule at some point in the past.

The stop in the present case demonstrates how this danger may manifest in police practice. The police had developed an interest in Mr. Arias for unrelated activity. Appellee's Brief at 9. However, they lacked the reasonable suspicion or probable cause necessary to effectuate a constitutional search of his vehicle. While they ultimately observed Mr. Arias commit a moving violation, they did not try to address the issue at the time. Instead, they performed a stop for a "drug investigation" based on a traffic infraction observed the day before. *Id*. at 10. In doing so, they attempted to evade the constitutional mandate of a justified

particularized search, and to reverse the usual order of reasonable suspicion giving rise to an investigation by manufacturing pretext from unrelated surveillance.

Had surveillance technology been used in this traffic stop, the result would be even more odious. Instead of relying on an in-person sighting of the traffic infraction, the police could have received a notification of the infraction from Flock. They could then set an alert to notify them the next time Mr. Arias was driving a particular car or in a particular neighborhood. When the alert triggered, the police could stop him and initiate a search of his vehicle. This would allow the police to initiate a stop based solely on characteristics that do not alone provide reasonable suspicion, like presence in a "high crime" neighborhood. *See United States v. Camacho*, 661 F.3d 718, 723 (1st Cir. 2011) (citing *Illinois v. Wardlow*, 528 U.S. 119, 124 (2000)). And, unlike the stop of Mr. Arias, the stockpile of infractions means officers would not need to rely on the luck of being present at the scene; police would simply have to flag Mr. Arias to the traffic surveillance system, sit back, and wait.

The question of whether a traffic stop conducted after a significant delay is reasonable is critical to determining whether police can take advantage of this kind of surveillance-based time-shifting. Specifically, this Court should consider the interaction between Massachusetts' objective test for traffic stops, the breadth of the traffic code, and the scale of modern traffic surveillance. These three factors,

combined, would create a system that subjects a large portion of the public to nearly blanket search and seizure authorization—in other words, a general warrant.

First, the objective standard opens the door to traffic stops being executed for pretextual reasons. As previously discussed, if police need merely point to a traffic violation to justify a stop, traffic surveillance systems effectively become bootstrapping devices. Under the Commonwealth's interpretation of the law, whenever a camera detects and logs a traffic infraction, traffic stop authorization would follow—and linger for at least twenty-four hours—and allow the police to initiate an on-demand seizure, even if for unrelated purposes.

Second, the breadth of the traffic code ensures that an incredibly broad population may be subject to a traffic stop. As Chief Justice Budd put it in *Long*, "[v]ery few drivers can traverse any appreciable distance without violating some traffic regulation." 485 Mass. at 739 (Budd, J., concurring) (internal citations omitted). This naturally includes many individuals who are, or in the future may be, of interest to the police for other reasons.

Third, traffic surveillance ensures that the breadth of the code manifests into a massive stockpile of evidence of traffic infractions. Not only does surveillance technology capture a greater volume of infractions, newer tools promise to automatically draw inference to tie these infractions to particular individuals or groups. Police thus have easy on-demand retrospective access to evidence of past

infractions for any individual of interest, with minimal legwork. In other states, search logs suggest that police have been routinely using this capability of Flock to conduct broad, unparticularized searches for evidence. *See* Begley et al., *supra* p.15. In short, if police want authority to stop a driver, surveillance technology will ensure that they can almost always find a traffic infraction to justify it.

Against this backdrop, the addition of a rule that allows for a significant delay between infraction and stop gives police an incredible power of discretion. The more tenuous the necessary proximity in time, the more power police would have to trawl through past violations in search of a "justification" for a traffic stop. At a certain point—a point *amici* believe is well short of twenty-four hours—this power becomes unconstitutional. The power to initiate a seizure *before* developing legally sufficient suspicion strongly resembles type of general warrant that the Fourth Amendment was meant to protect against. *See McCarthy*, 484 Mass. at 498–99 ("The surveillance implications of new technologies must be scrutinized carefully, lest scientific advances give police surveillance powers akin to these general warrants."). Here, a stockpiling of pretexts for investigatory stops achieves the same end as a blanket license to investigate individuals without a threshold reasonable suspicion.

In summary, traffic stops should be cabined to the circumstances that justify them: the immediate need to address an ongoing safety issue. Where the police merely have an interest in a person, and no evidence that would allow them to initiate

a stop or obtain a warrant for a search, they should not be permitted to turn every traffic infraction into an evidentiary fishing expedition. The alternative—broad authorization to conduct pretextual stops based off of past infractions—would turn already troublesome surveillance networks into a bottomless well of invasive, in-person seizures.

CONCLUSION

For the foregoing reasons, *amici* respectfully request that this Court reverse the judgment of the lower court and hold that, absent exceptional circumstances not present here, a twenty-four-hour delay between observing a traffic violation and conducting a traffic stop renders the stop unconstitutional.

Dated: November 12, 2025

Respectfully submitted,

/s/ Mason A. Kortz

Mason A. Kortz (BBO #691257)
HARVARD LAW CYBERLAW CLINIC
1557 Massachusetts Avenue, 4th Floor
Cambridge, MA 02138
(617) 495-2845
mkortz@law.harvard.edu

Counsel for Amici Curiae[17]

[17]*Amici curiae* thank Fall 2025 Cyberlaw Clinic students Alex Peile, Jenny Guzdial, and Juvaria Shahid for their valuable contributions to this brief.

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 17(c)(9) of the Massachusetts Rules of Civil Procedure, I, Mason A. Kortz, hereby certify that the foregoing **Brief of Mailyn Fidler and the Electronic Privacy Information Center in support of Appellant and Reversal** complies with the rules of court that pertain to the filing of amicus briefs, including, but not limited to:

Mass. R. A. P. 16(e) (references to the record);
Mass. R. A. P. 17(c) (cover, length, and content);
Mass. R. A. P. 20 (form and length of brief); and
Mass. R. A. P. 21 (redaction).

I further certify that the foregoing brief complies with the applicable length limitation in Mass. R. A. P. 20 because it is produced in the proportional font Times New Roman at size 14 points and contains 4,686 total non-excluded words as counted using the word count feature of Microsoft Word 365.

Dated: November 12, 2025

Respectfully Submitted,

/s/ Mason A. Kortz

Mason A. Kortz, BBO #691257

COMMONWEALTH OF MASSACHUSETTS

SUPREME JUDICIAL COURT

No. SJC-13816

COMMONWEALTH OF MASSACHUSETTS,
Plaintiff-Appellee,

v.

JOSE ARIAS,
Defendant-Appellant.

CERTIFICATE OF SERVICE

Pursuant to Mass. R. A. P. 13(e), I, Mason A. Kortz, hereby certify, under the penalties of perjury, that on this date of November 12, 2025, I have made service of a copy of the foregoing **Brief of Mailyn Fidler and the Electronic Privacy Information Center in support of Appellant and Reversal** in the above captioned case upon all attorneys of record by electronic service through eFileMA.

Dated: November 12, 2025

Respectfully Submitted,

/s/ Mason A. Kortz

Mason A. Kortz (BBO #691257)
HARVARD LAW CYBERLAW CLINIC
1557 Massachusetts Avenue, 4th Floor
Cambridge, MA 02138
(617) 495-2845
mkortz@law.harvard.edu