ACLU
AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175
www.riaclu.org
info@riaclu.org

November 17, 2026

VIA MAIL AND EMAIL

Colonel Darnell Weaver
Rhode Island State Police
311 Danielson Pike
North Scituate, RI 02857

Dear Colonel Weaver:

We understand that the intent of the recently proposed Statewide Automated License Plate Reader (ALPR) policy is to provide uniform standards around the state and serve as a model for future legislation. In the absence of a ban on the use of ALPRs, which we strongly support, our organization has long advocated for a strong statewide law reining in this invasive surveillance technology. Upon comprehensive review of this proposed policy, however, we believe it requires significant revision before it is sufficiently robust to warrant consideration by a legislative committee or as a standard that cities and towns should consider implementing.

The proposed policy draws heavily from existing Rhode Island State Police (RISP) policy, with a few additional provisions modeled on standards in effect for Providence Police. In late 2025 and early 2026, when RISP launched its effort to set up a network of 39 cameras throughout the state, we testified against that program and shared our concerns with municipal councils asked to participate in it. Many of our comments about this latest proposed policy may therefore be familiar, as the concerns we expressed about the RISP guidelines remain unaddressed in this latest proposal.

The invasive impact of this technology on Rhode Islanders' privacy rights is obvious. As a result, we have consistently opposed these surveillance devices in our communities since the first ALPR cameras were installed – without any public discussion – in Cranston, Woonsocket, and Pawtucket in 2021. In the past five years, the dangers of a surveillance state promoted by this technology, and its repeated documented abuse and misuse, have only heightened both our concerns and the legitimate privacy concerns of the public. Time has only made clearer the need for a strong state law restricting the use and expansion of ALPRs in Rhode Island.

With this as a backdrop, we urge favorable consideration of our analysis of the proposed policy and our suggested changes. Given the significant capabilities of these systems, the policy's shortcomings warrant careful attention and modification before serving as a model for legislation or ordinance. In light of the detailed and repeated testimony and correspondence we have had with police departments and public bodies over this technology, we do not seek here to rehash all of the arguments we have made for banning these cameras, although we would be happy to share that information. Instead, we take at face value the Governor and police representatives' position that they seek to establish meaningful safeguards to reduce the serious privacy implications of this

technology and its potential misuse. With that understanding, we hope our comments will prompt recognition of the need for a much stronger policy for those municipalities and police forces that choose to continue to make use of this intrusive surveillance technology.

Our analysis begins with five broad and fundamental concerns with the proposed policy, and then proceeds to address some more specific issues:

1. **Section III. Definitions. "Valid Law Enforcement Purpose" Definition.** Section II states that the policy's goal "is to utilize ALPR technology to capture and store digital license plate data and images for valid law enforcement purposes while recognizing the established privacy rights of the public." However, a "valid law enforcement purpose" is defined incredibly broadly in the policy, covering such open-ended goals as "the prevention of crime" and "ensuring the safety of the public." This essentially allows the ALPR system to proactively track just about any individual or groups of individuals with the most meager of rationales for virtually any suspected criminal offense, as police can almost always justify access to the system based on such open-ended standards. It is essential that any policy make its use much more limited in scope for the types of crimes that authorize access to this data.[1] To offer an example, we refer to the more focused standards contained in legislation to regulate Flock Safety cameras that was introduced this year.[2] Put simply, the policy should list the particular situations when access to the data *is* allowed rather than when it is not.

   The proposed policy's lack of constraints on the circumstances when the technology can be used is apparent elsewhere. For example, Section IV(B) purports to restrict ALPR use to three outlined purposes. But subsection (a) simply repeats the broad term "valid law enforcement purpose." It then offers an example: "*such as* being used as part of a criminal investigation into an alleged violation of state or federal criminal law where there is reasonable suspicion that a crime was committed." (emphasis added) But the phrase "such as" gives away the game that this section provides no real guiding limit as to what constitutes a "valid law enforcement purpose."

   Similarly, Section IV(D)(2) specifies seven situations when ALPR data can be used, but it is explicitly "not limited to" the particular scenarios listed. In short, combined with the largely unrestricted definition of "valid law enforcement purposes" noted above, it means that the data can be accessed and used (and misused) for just about any purpose even as the policy tries to ambiguously suggest otherwise.

   Put another way, even if one does not take issue with the specifically listed purposes of data use, any suggestion they provide of limiting the use of ALPRs is illusory.

[1] We acknowledge and appreciate that scattered throughout the policy are various restrictions on use of the system for *civil or other non-criminal purposes* (e.g., harassment or personal use), but our comments refer to the broad use of the cameras for virtually any activity that can be considered criminal in nature, however minor.

[2] H 8077, https://webserver.rilegislature.gov/BillText/BillText26/HouseText26/H8077.pdf.

2. **Section III. Definitions. "Automated License Plate Readers (ALPRs)" Definition.** The policy defines ALPRs as a "device that uses cameras and computer technology to convert *the images of license plates* to electronically readable data and compares digital images to lists of known information of interest." (emphasis added) This ignores the fact that the cameras capture much more than license plate data. As the policy statement in Section II notes, ALPRs also allow for the detection of the "vehicle make, model, color and unique identifiers." One of those "unique identifiers" not specified is the ability to track vehicles by their bumper stickers, a capability that raises unique First Amendment concerns.

   Even more disturbing, the policy does not prevent the use of ALPRs for taking photographs of drivers and their passengers. Despite the many misleading assertions police have made (and that this policy implies) that ALPRs photograph only the rear of motor vehicles, revelations in a recent lawsuit filed against the Cumberland Police Department show that this is simply not so. In that case, a Flock Safety camera took facing-forward photos of the inside of a vehicle and the person driving it. Ironically, the ALPR photo led to the unlawful arrest of an individual. Nothing in the proposed policy would prevent use of ALPRs to photograph people, not just vehicles, nor would it ultimately prohibit the incorporated use of even more intrusive measures in the future, such as facial recognition technology.

3. **Section IV(H)(2). Security of Information.** The policy states that "unless preserved as part of an investigation, ALPR data shall purge no later than 30 days after the data was captured." This timeframe is problematic for at least two reasons.

   First, by allowing non-investigative surveillance data to be kept for up to a month, the policy sets a standard much longer than the seven-day default timeframe for retention that was recently set by Flock Safety itself. In other words, the policy proposes a data retention period more than four times longer than the company's own recommended time period. Considering Flock Safety's dubious record when it comes to protecting privacy and promoting transparency, a police policy that is even less protective is worth highlighting. When weighing the interests of law enforcement against the privacy interests at stake, any policy or law setting standards for ALPR use greater than the company's default period fails to set an appropriate balance.

   Second, this provision provides no guidance on the scope of data that can be maintained when preservation is allowed "as part of an investigation." For example, if the police are conducting a murder investigation and hoping they will be able to find the perpetrator's vehicle using ALPR, can the police maintain every piece of data from every camera in the municipality while the investigation proceeds, or will they be limited to keeping data only from the one or two cameras nearest the scene of the crime? Absent any guidance, the policy could allow for indefinite, and almost perpetual, use of significant amounts of ALPR data notwithstanding this provision's implicit suggestion to the contrary.

4. **Section VIII(1). Violations.** The proposed policy's penalties for violations are distressingly inadequate. It provides that any officer found to have impermissibly used the system "may" have their use of the ALPR system "temporarily or permanently suspended." Thus, an officer who has improperly accessed ALPR data could still be authorized to use

the system despite a blatant breach of trust. In addition, the policy claims that officers who misuse the system may be subject to criminal prosecution or civil liability. But absent a law that actually makes misuse of this system a crime or establishes a civil cause of action, this assurance seems largely meaningless. Finally, in light of the proposed policy's meager auditing measures (discussed in more detail below), the odds of catching an officer misusing the system will remain slim to none.

5. **Failure to Constrain Further Technological Uses of ALPRs**. The policy is as notable and ineffective for what it does *not* say as for what it does. On a regular basis, Flock Safety announces new and expanded capabilities of the system, such as being able to: flag multiple vehicles the system believes are associated with each other; search by sounds; search by driving-behavior predictive analysis; and, depending on the camera model, users can even search by a person's clothing. There is absolutely nothing in the policy that seeks to limit the cameras' capabilities to what law enforcement spokespeople consistently try to sell the public: that they merely capture license plate data and therefore raise minimal privacy concerns. A policy that purports to rein in the privacy intrusions of the ALPR system but fails to take into account the possible broader – and even more intrusive – uses of the system offers little assurance to the public that their privacy is being protected.

Below we offer some additional amendments to the model policy. We have sorted our concerns into four categories: Vagueness, Access, Enforcement, and Transparency and Use.

Vagueness: The items from the policy detailed below are too broadly written and thus undermine the intent of creating clear and limited safeguards around these camera systems.

1. **Section III. Definitions. "ALPR Data" Definition.** The policy defines ALPR data as "scan files, alert data, and any other documents or data generated by, or obtained through, utilization of the ALPR system." As with the definition of ALPRs, as noted above, the definition of "ALPR data" fails to capture the full scope of information collected by the system. We believe that the definition should include an additional sentence to avoid any ambiguities about the scope of the data collected: "This includes, but is not limited to, GPS coordinates, date and time, photograph, license plate number, and any other data captured by, derived, or inferred from any automatic license plate reader system, such as the vehicle make, model, color, bumper stickers, and other automobile characteristics." Simultaneously, as also noted above, the policy should add specific limits on any additional types of data collection.

2. **Section IV(C)(3)(c). Entry and Verification into the ALPR System.** This section requires that information entered in the system contains at a minimum: "1) related case number; and 2) short synopsis describing the nature of the originating call." Based on vague audit log entries we have seen in the past, we believe that the "short synopsis describing the nature of the originating call" should include the specific basis for the initiation, and general and generic reasons like "investigation" should be prohibited. In order to provide proper oversight and identify instances of misuse, the synopsis must be as specific as possible.

Additionally, this section is modeled off the Providence Police policy. That policy also requires vehicle and suspect information entered into the system to include the "entering department member's name." We believe this should be included in the statewide proposed policy.

3. **Section IV(G)(5). Accountability and Safeguards.** This section states that "every ALPR Detection Browsing Inquiry must be documented by both the associated law enforcement agency case number, or incident number, and a reason for the inquiry." As noted prior, when the system is queried, the policy should require a specific explanation of the purpose of each inquiry that is sufficient to provide meaningful oversight over the system's use.

Access: Regulating who has access to the data that is collected is a critical part of ensuring Rhode Islanders' privacy rights are protected. Each of these suggested changes narrow or clarify who can access and use data collected by the ALPRs.

1. **Section IV(A)(1). ALPR Administrators.** This section states that, "Only properly trained sworn officers, analysts, police dispatchers, and telecommunicators are allowed access to the ALPR system or to collect ALPR information." Although this section requires training, it authorizes access to the system to a broad range of department personnel. Rather than meaningfully restricting access, it effectively permits access by almost any employee as long as they are "trained." Instead, access should be further restricted. In fact, recent guidelines created by the International Association of Chiefs of Police encourage limiting access to ALPR systems to only those staff members who need it for their jobs, and "promptly removed when an individual's duties no longer require it."[3] The proposed policy should follow that guidance.

2. **Section IV(D)(2). Authorized Collection, Purposes and Use of ALPR Data/Guidelines for Use**. Subsection (f) allows use of this technology to "protect participants at special events." We are concerned that this risks permitting law enforcement intrusion into public spaces that will create a chilling effect on constitutionally protected activities. Individuals who believe they may be monitored are often less likely to freely exercise their rights, including expressing their views at, or attending, protests or public gatherings, making somewhat questionable the guarantee elsewhere in the policy that the system will not be used to infringe First Amendment rights.

3. **Section IV(F). Authorization to Share ALPR Information.** This section seeks to partially restrict a department's ability to share information, but the proposed restrictions are incomplete. At a minimum, this provision should be amended to include restrictions on sharing the information for any of the prohibited uses outlined in Section IV(E). As it currently stands, restrictions on sharing only apply to immigration information, despite the fact that the preceding section prohibits use of the system for other reasons, including personal use, interference with First Amendment rights, or the enforcement of anti-abortion laws.

[3] https://www.washingtonpost.com/technology/2026/10/21/their-police-jobs-ended-they-kept-using-flocks-vast-surveillance-network/

4. **Section IV(G). Accountability and Safeguards.** Subsection (G)(1) states that "all non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law." We are concerned about the relationship between this provision and the preceding section, IV(F)(2), which states that "departments are prohibited from sharing, disseminating, forwarding, or otherwise providing access to any data, images, or alerts to any third party that is not a law enforcement agency." Seemingly, Section IV(G)(1) appears to contemplate processing non-law enforcement requests, whereas IV(F)(2) expressly prohibits access by non-law enforcement.

   Additionally, subsection (G)(4) mentions the need for third party law enforcement agencies to sign "an appropriate MOU." But neither this section nor Section IV(I)(1), which also mentions the need for an MOU, specifically requires the third party to confirm it will abide by all of the restricted uses and sharing limitations applicable to Rhode Island law enforcement agencies subject to this policy. That is a large gap in protection. This provision and the current MOU draft should be made more explicit, making clear that by signing the MOU, the signing agency is agreeing to all of the restrictions contained in the policy.

5. **Section IV(I). Releasing ALPR Data.** This section lists the circumstances under which ALPR data may be shared. Subsection 5 allows data to be shared "with an ALPR vendor for maintenance or quality assurances purposes." We believe that this sentence should clarify that the data can be provided to the vendor only for those two reasons, and solely to the extent necessary to carry out those functions.

   In addition to the circumstances listed in this section for when data can be released, there is an additional one that deserves inclusion in the name of transparency: in the absence of an investigatory or other legitimate purpose, an individual should have a means of learning whether information about *themselves* or their vehicle has been collected or accessed through this system.

Enforcement: Holding law enforcement officials who misuse the system accountable is an important part of regulating this surveillance technology. We urge one clarifying amendment to the role of ALPR administrators set out in the policy.

1. **Section IV(A)(3). ALPR Administrators.** This section requires "ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws." This section should be amended to include the words "and this policy" at the end of the sentence. Compliance with applicable law alone falls short since any privacy restrictions that apply to this information will mostly be the result of the limits set by this policy, not by statute.

Transparency and Use: For the model policy to be robust, the approved use of these systems must be extremely transparent. Additionally, how the data can be used, and when, cannot be open to interpretation or confusion. As such, we suggest edits to make sure the system is transparent and there is no doubt who can and should be able to access the system or the data.

1. **Section IV(C)(2). Entry and Verification into the ALPR System.** This section governs a police department's verification process of an ALPR alert. The section says, "The officer *should* verify an ALPR response through the Rhode Island Law Enforcement and Telecommunications System (RILETS) before taking enforcement action that is based solely on an ALPR alert unless exigent circumstances exist." (emphasis added). We urge that "should" be replaced with "shall."[4]

2. **Section IV(E)(1). Prohibited Use.** While we support creating a strong policy prohibiting the inappropriate use of these cameras, we question some of the language in this section. The policy states that ALPRs may only capture plates exposed to public view, but it includes vehicles on private property whose license plates are visible from public areas, such as driveways or business parking lots. We find this troubling, given that Flock Safety markets its technology as capturing vehicles as they pass via motion detection.[5] This provision seems to expand the scope of permissible surveillance beyond the public roadways that one would expect from the system.

3. **Section IV(G)(7). Accountability and Safeguards.** We appreciate that the policy requires police departments to publish transparency portals providing important information related to these cameras. However, we know that the metrics required by the policy are not all the metrics that these portals can include. Instead, the portals should be required to include all information available for display, including a list of the other agencies that the law enforcement agency receives information from, the camera alert activity, and a public search audit. These portals should be conspicuously posted on the police department's website, making information easy to find.

4. **Section IV(I)(1). Releasing ALPR Data.** This section requires an ALPR administrator to approve a law enforcement request for access and to retain the approved request on file. These approved requests should be designated as being publicly available. This availability would provide meaningful oversight from the public into a department's ALPR use and access practices.

5. **Section VII. Audits.** This section requires the ALPR administrator to conduct a quarterly audit of the system by sampling ten browsing inquiries. If this is meant to be an oversight mechanism to find abuses of the system, it is woefully inadequate. We strongly support codification of an auditing requirement into law, but sampling ten inquiries every three months is almost pointless. In one month alone, a Cranston police organizational audit detailing the number of license plates searched exceeded 150 pages. A network audit from the same month in Cranston demonstrated that its cameras were queried by outside agencies over 400,000 times.

---

[4] In the same section, a line reads, "officers will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been *publicated*." (emphasis added). We assume this unknown word is an error; the Providence Police policy that this section is based on uses the word "validated."

[5] https://www.flocksafety.com/faq

Miscellaneous.

1. **Section IV(E)(6). Prohibited Use.** As a technical matter, to avoid any conflict with federal immigration law, the policy should contain the following compliance language:

   > "Nothing in this chapter prohibits or restricts any official from sending to or receiving from federal immigration authorities, information regarding the citizenship or immigration status, lawful or unlawful, of an individual pursuant to Sections 1373 and 1644 of Title 8 of the United States Code."

2. **MOU.** As noted above, we support the requirement that an MOU be signed before any information is shared between agencies. However, the MOU should be made more explicit in requiring the signing agency to agree to all of the restrictions contained in this policy.

While these suggested revisions are admittedly extensive, we believe they are essential if the policy's goal is to ensure that use of this surveillance technology appropriately balances safety interests and the privacy rights of this state's residents.

We thank you for your consideration of these comments and hope they will be given favorable consideration. I remain available to answer any questions you may have about them.

Sincerely,

Madalyn McGunagle

Madalyn McGunagle
Policy Associate

cc: Governor Daniel McKee
Governor-Elect Helena Foulkes
Colonel Oscar Perez, Providence Chief of Police
Rhode Island Police Chiefs Association
Rhode Island League of Cities and Towns
Rhode Island Police Accreditation Commission