M1

ACLU
AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175

January 28, 2026

VIA EMAIL

Members of the Bristol Town Council
Bristol Town Hall
10 Court Street
Bristol, RI 02809

Dear Town Councilors:

We thank the Council for the opportunity to present our perspective on the proposed Rhode Island State Police (RISP) policy concerning the use automated license plate readers (ALPRs), the proposed Memorandum of Understanding (MOU) between the RISP and third parties who receive their data, and correspondence from Chief of Police Kevin Lynch. Notably, this same proposal was unanimously rejected last night by the Portsmouth Town Council.

We have several comments and concerns regarding both the RISP General Order-80G and the proposed MOU. They are as follows:

RISP General Order 80G:

- **Section II (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." ALPRs are powerful tools that capture much more information than just digitized license plate numbers, and the shared network allows for significant tracking capabilities. Because of the power of these systems, the definition of ALPR data should be expanded to explicitly reflect the full scope of data collected. 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."

- **Section II (Definitions). "Valid Law Enforcement Purpose" Definition.** Section IV(B)(2) states that "all ALPR queries shall be in furtherance of a valid law enforcement purpose." However, a "valid law enforcement purpose" is defined extremely broadly in the policy, to cover 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. It effectively grants access to these systems for any reason, and should be much more limited

in scope. For a model, we refer to the legislation to regulate Flock Safety cameras that was introduced last year, which is much more focused.

- **Section IV(B)(3). Purposes of Collection.** While this portion of the policy purports to specify the situations when ALPR data can be used, it is explicitly "not limited to" the particular scenarios listed. Combined with the open-ended definition of "valid law enforcement purposes" noted above, it means that the data can be used (and misused) for just about any purpose.

  While we do not take issue with most of the listed purposes of data collection, we are concerned that they are ultimately meaningless. Thus, for example, while the data can be used to locate witnesses of "violent" crime, the rest of the policy language actually allows the ALPR system to be used to locate witnesses for virtually any reason. We are also concerned about the lack of a definition as to what constitutes "critical infrastructure" and how generating license plate data would protect it.

  Additionally, we worry that allowing use of this technology for "special events" 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 or attending protests or public gatherings, making somewhat questionable the guarantee elsewhere in the policy that the system will not be used to infringe on First Amendment rights.

- **Section IV(C)(1). "Prohibited Users."** 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 that it includes vehicles on private property whose license plates are visible from public areas, such as driveways or business parking lots. We find this particularly troubling, given that Flock Safety markets its technology as capturing vehicles as they pass via motion detection.[1] This provision seems to expand the scope of permissible surveillance beyond what is publicly represented.

  We commend the RISP for their commitment to prohibiting the sharing of sensitive ALPR data with Immigration and Customs Enforcement (ICE) or similar agencies (but see our comments below on Section IV.D.) However, based on disclosures of misuse of ALPRs elsewhere, we believe at least one other specific restriction should be added. Specifically, data should not be shared with third parties or federal agencies for purposes of enforcing non-Rhode Island restrictions on access to reproductive or gender-affirming healthcare. Following reports that authorities used ALPR data to find a woman who was suspected of having an abortion,[2] we are concerned that this data could be used by third parties to target those individuals who are seeking care in Rhode Island.

[1] https://www.flocksafety.com/faq
[2] https://www.eff.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-missing-person-it

- **Sections IV(D)(2) and (G)(1). Sharing and Release of ALPR Data.** We support the stated restriction in Section (D)(2) on sharing ALPR data with third parties that have not entered into an MOU with RISP. But, at least for a few reasons, this restriction amounts to much less than it might seem. First, we are concerned about how this provision interacts with Section IV(G)(1), which permits access to this data by other law enforcement agencies. Neither section clearly states that other law enforcement agencies seeking access to this data are considered third parties and required to sign an MOU.

  Further, neither section makes clear that the required MOU includes all of the restrictions on use that are contained in the RISP policy. Because of this gap, those agencies could in fact receive ALPR data and share it with ICE or other entities without being subject to the disclosure restrictions in the MOU, use it to infringe on First Amendment rights, and so on. That is, the policy does not make clear that any MOU signed between the RISP and a third party must include all of the use restrictions listed in Section IV(C) and elsewhere concerning prohibited uses. Our concern is further compounded by Section IV(E)(4), which allows ALPR data to "be released to other authorized and verified law enforcement officials and agencies" for undefined "legitimate law enforcement purposes," subject to the approval of the ALPR administrator.

  An even bigger loophole appears in Section IV(G)(1), since it additionally allows the sharing of data with other agencies "as otherwise permitted by law." Since there are no statutory restrictions on the sharing of ALPR data in Rhode Island, we believe this section gives unbridled discretion to RISP to share information notwithstanding all the purported restrictions appearing in the policy. In short, we believe that these sections create ambiguities about who is subject to the MOU's restrictions and must be clarified to ensure that all entities receiving this data are subject to the same data-sharing limits.

- **Section IV(E)(2). Accountability and Safeguards.** This section requires ALPR data accessed on mobile devices or computers to be protected by a password protected login system capable of documenting all access. While we support these safeguards, the policy does not address how long this data remains stored on individual devices or whether deletion is automatic. Because of this ambiguity, this section should include a clearly defined retention period for ALPR data stored on these devices.

- **Section IV(F)(2). Security of Information.** The policy states that "Flock automatically purges captured plate data after 30 days." However, this section does not make clear that RISP itself, as the owner of the data, is also purging the data from its systems within this time period, or that any agency or third party that has received the data must also delete the data after 30 days. Second, we would note that 30-day data retention is the standard time in Flock Safety contracts, but the timeframe actually can vary based on state laws. For example, New Hampshire retains ALPR data for three minutes, and Virginia for 21 days.[3] Finally, relying on Flock's current 30-day policy to set the standard for RISP ignores the fact that Flock could change its practice at any time and decide on a longer retention rate.

[3] https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes

Memorandum of Understanding (MOU) between RISP and the Town of Bristol:

- **Party Ambiguity.** Although the MOU is entered into by RISP and the Town of Bristol, the document only refers to the "outside agency." We are assuming that this is Bristol, though the document does not define what the "outside agency" is. We are concerned by this ambiguity as it raises concerns about accountability regarding which entity is bound by the agreement. It should also specify that Bristol itself cannot share data collected by the RISP camera with any other agencies, but rather that third parties would need to go through RISP to do so.

- **Authorized Use.** The MOU permits ALPR data to be used "solely for law enforcement and public safety purposes, including but not limited to criminal investigations, active searches for stolen vehicles, missing persons, or suspects in serious crimes." For all the reasons we have expressed in raising concerns about the breadth of the RISP policy, we have concerns about this similarly broad language and the way it tends to undermine the true availability of meaningful restrictions on the use and sharing of ALPR data.

Correspondence from Chief Lynch to the Council:

We do not wish to unduly prolong this letter, but we would like to briefly respond to just a few of the comments offered by Chief Lynch to the Council:

- In his response, Chief Lynch wrote that "Flock does not share customer data with any federal agency," and that ICE and other federal agencies "cannot directly access Flock cameras or data." As we previously stated, we commend the effort to limit the amount of license plate data shared with ICE and other federal agencies. However, our concern is that the nationwide data sharing capability of this system still allows for ICE or other federal agency access to this information. ICE can ask, and has in the past asked, other law enforcement agencies to query the system on their behalf.[4] Additionally, Flock only recently paused a pilot program which granted ICE, Customs and Border Patrol, the Secret Service, and other federal agencies access to camera data.[5] We are concerned that pausing pilots like these are only temporary and would open up federal agency access to a wide swath of sensitive information.

- In addressing the lack of legislatively established limits on these systems, Chief Lynch stated, "attempts have been made (like H 7507 in 2022)" and that "the RIPCA has long supported legislation to establish similar guidelines" as to what are already in police policies regarding ALPRs. We would like to add that legislation to rein in this technology has been introduced every year subsequent to 2022, and police chiefs have expressed their opposition to each of them, including in 2022. Any alternative legislation that the police have expressed a willingness to support would, to the best of our knowledge, incorporate

[4] https://www.404media.co/feds-used-local-cops-password-to-do-immigration-surveillance-with-flock-cameras/; https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/

[5] https://www.404media.co/ice-secret-service-navy-all-had-access-to-flocks-nationwide-network-of-cameras/; https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_flock.pdf

the many deficiencies we have cited in this letter that are contained in the RISP policy, and therefore provide little protection at all.

Many other states have already passed substantive laws regarding ALPR use. We would note that had any of the Rhode Island bills introduced in the last few years become law, nothing in them would have prevented or impeded their use in the investigation of serious crimes, including the horrific shooting at Brown University.

- While Chief Lynch claims that one of Flock Safety's "built-in privacy protections" is that "LPRs do not track vehicles continuously," that is precisely the goal of installing more and more of these surveillance cameras across the state. Each data point generated by these cameras can, through the shared networking of the system, be compiled together to create a map of where someone has been during the day, or a week or a month.

Thank you for the opportunity to present our perspective and for your consideration of this matter. We would be happy to answer any questions you may have.

Sincerely,

Madalyn McGunagle

Madalyn McGunagle
Policy Associate

cc: Police Chief Kevin Lynch, Chief of Police
Steve Contente, Town Administrator