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 10, 2025

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

VIA EMAIL

Dear Town Councilors:

Item F3 on the Town Council meeting agenda for Wednesday, November 12, 2025, concerns a request from the Rhode Island State Police (RISP) to approve their installation of "at least one" Flock Safety camera in the town of Bristol. We are writing to express our organization's deep concerns regarding the proposed installation of any Flock Safety automated license plate reader (ALPR) camera systems in your town.

While the ACLU of Rhode Island certainly understands the importance of public safety, the approach to safer communities cannot and should not include the usage of technologies – like these cameras – which raise serious privacy issues, carry the clear potential for expanded surveillance, and are implemented with no statutory safeguards in place. We therefore urge you to reject the request of the RISP.

Our organization has substantive concerns about the actual technology of these cameras, but we are just as distressed by the possibility that these surveillance systems are being implemented without the concurrent introduction of statutory safeguards and limitations for their use. We wish to provide some context as to why the ACLU believes your municipality should reject the request for installation of these cameras and, alternatively, demand safeguards governing the use of these systems if approved.

• **The cameras capture more than license plate numbers**. Rhode Island's use of other ALPR systems – such as those utilized for tolling purposes or to monitor traffic patterns – have generally been contained to capturing only the license plate on a vehicle, and only for a specific and narrow purpose. When the implementation of Flock Safety cameras in other municipalities began to occur, police representatives initially assured the average motorist that they need not be worried because police are alerted only if a car's license plate number matches information in a federal national criminal database, known as the NCIC, or Amber/Silver Alert systems.

But leaving aside the well-known inaccuracies of the NCIC database and the problems that alone can cause, it is clear now – through the admission of the police departments – that these systems are not as narrowly tailored as residents may expect or anticipate. Concerns about overreach are only compounded by the acknowledgement of the expansive surveillance properties contained in, and the invasive measures allowed by, these technologies.

Investigators may input a wide variety of vehicle characteristics into the system which range far beyond license plates. In a now-deleted section of Flock Safety's website, the company once flaunted that its surveillance system allowed police to search by "vehicle type, make, color, license plate state, missing/covered plates, and other unique features like *bumper stickers*, decals, and roof racks." (emphasis added) These capabilities are extraordinarily invasive, extending far beyond what most people imagine when they hear the term "automated license plate reader."

Further, as the reference to "searches" suggests, the system does not merely operate passively. Police can input any license plate number – and presumably vehicle characteristics such as those noted above – and obtain information about a vehicle's whereabouts, if captured by a camera, for the preceding 30 days. These searches are not confined solely to a single jurisdiction. Searches include images from any future Bristol cameras, from any other municipality participating in the regional sharing network, and even camera systems located far outside Rhode Island.[1]

In fact, recent reports have revealed that Customs and Border Protection (CBP) has conducted searches of Flock Safety's ALPR databases across the country to enforce the Trump Administration's anti-immigrant agenda.[2] At the same time, police departments have reportedly performed Flock lookups on behalf of Immigration and Customs Enforcement (ICE), which did not have its own access.[3] Even if RISP itself would turn down ICE requests for information, any other police department in the country with access to the department's camera data could share it instead. In another case, a police department in Texas used Flock's nationwide network to search more than 83,000 ALPR cameras to locate a woman suspected of having an abortion.[4]

Despite assurances that the alert system only triggers for vehicles linked to criminal activity and that innocent motorists thus have nothing to fear, one would assume that camera alerts would be few and far between. Yet, according to the transparency portal[5] set up for the Cranston Police Department, to give one example, those cameras have taken photographs of nearly *half a million cars* within the last thirty days. Each of those images remains available for police searches for that same timeframe.[6]

At the same time, the positing that these cameras operate solely based on the visual capturing of information is misleading. Flock Safety's website advertises the ability to not only search by the aesthetic characteristics listed above but additionally by "audio evidence" and "contextual evidence," which includes such evidence as "screeching tires" and "associated vehicles,"[7] implying that these systems capture both audio and video, and utilize artificial intelligence to determine which vehicles in a certain area may be linked to one another. Both of

---

[1] For example, Woonsocket, RI shares camera data with many municipalities including Houston, TX. *See* https://transparency.flocksafety.com/woonsocket-ri-pd

[2] https://www.404media.co/cbp-had-access-to-more-than-80-000-flock-ai-cameras-nationwide/

[3] https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/

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

[5] Transparency portals are online portals created by Flock Safety to show the public certain metrics in the use of these systems. If this RISP camera is approved, a transparency portal should be created.

[6] https://transparency.flocksafety.com/cranston-ri-pd

[7] https://www.flocksafety.com/

these uses, beyond the already invasive capabilities of video capturing, would be a profound overreach of this technology and invite over-policing and an inappropriate broadening of surveillance techniques.

• **It is almost inevitable that the use of these cameras will expand over time to engage in more, and more intrusive, types of surveillance**. The history of surveillance technology in this country – from wiretaps to stingrays to cameras to drones – has been a history of ever-growing uses, and those expanded uses are then used to justify and normalize even greater intrusions on privacy. One common argument used to dismiss privacy concerns about installing these cameras is the widespread prevalence of surveillance in other areas. Not only does this gradually erode our expectations of privacy, but it also normalizes these surveillance processes.

Flock Safety's cameras exemplify this "mission creep." In addition to the standard technology that Flock Safety provides, the company announced the availability of "advanced search" features for its camera systems that will:

- Allow police to upload a picture of a vehicle from any source and then perform a search to see if any of the cameras have seen it;
- Allow police to enter a license plate number, and then search cameras to find vehicles that frequently travel with that vehicle, to "help identify accomplices to crimes"; and
- Give police the ability to search for vehicles that have been in multiple specified locations recently.[8]

Even if not being used in these more expansive ways today, the potential capabilities of this program are not as narrow as simply identifying and cross-checking license plate numbers, and nothing prevents expanded uses in the future. The chilling effects of the ability to track individuals in all these manners cannot be understated.

We are also concerned that installation of an RISP-controlled camera will, in turn, encourage the Town of Bristol to seek camera systems of their own, fueling continued surveillance concerns for Bristol residents. Additionally, it is unclear from the RISP's request how a Flock Safety camera and the data it collects will impact the Town of Bristol and its residents, especially considering the data-sharing issues with CBP and ICE, as mentioned above.

• **In the absence of legislatively established limits on their use, the privacy rights of the public remain at the complete discretion of the police department and a private company, which can change their policies at any time.** No matter what assurances of privacy are given in policy – by either a police department or Flock Safety – there are no meaningful constraints on their ability to change the rules at any time. Today we may be told, for example, that all photos will be destroyed after 30 days, but nothing prevents the agencies or the company six months from now from extending it to 60 days, a year, or a decade. The same is true for any other "safeguards" offered exclusively by police departmental policy or Flock Safety guidelines.

[8] https://www.govtech.com/biz/flock-safety-gives-users-expanded-vehicle-location-abilities

When police surveillance techniques like ALPRs are promoted, they often imply a false choice between public safety and privacy. But public safety is the result of community-based tools and systems that directly and tangibly support residents – it is not, and has never been, a consequence of indiscriminate 24/7 surveillance. To suggest that such surveillance technology is only a threat to those committing crimes is dismissive of the legitimate privacy concerns that all residents have and particularly ignores how police surveillance over the decades has often targeted communities in a racially discriminatory manner.

While the above are detailed concerns directly related to Flock Safety's cameras and the specific implementation of them in your municipality, we wish to emphasize that all surveillance technology has the capability to encourage, intentionally or not, more aggressive and unduly invasive policing and to foster community distrust in policing systems. For all these reasons, we urge the Town Council to reject the RISP request to install a Flock Safety camera in Bristol. Instead, the Town should consider enactment of an ordinance that promotes community engagement, oversight, and extensive transparency for any potential law enforcement surveillance technology. We would be happy to offer recommendations in that regard.

Thank you for your consideration of these concerns. If you have any questions about our views, please feel free to let us know.

Sincerely,

Madalyn McGunagle
Policy Associate

cc: Col. Darnell Weaver, RISP
Police Chief Kevin Lynch, Chief of Police
Steven Contente, Town Administrator