



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

June 3, 2026

Members of the Little Compton Town Council  
Town Hall  
40 Commons; P.O. Box 226  
Little Compton, RI 02837

VIA EMAIL

Dear Town Councilors:

We write to the Town Council to express the ACLU of Rhode Island's serious concerns regarding a pending request from the Little Compton police department to install a Flock Safety automated license plate reader (ALPR) in the Town. While we certainly understand the importance of public safety, the approach to safer communities cannot and should not include the continued usage of technologies – like these cameras – which raise significant privacy issues, are implemented with strikingly no statutory safeguards in place, and carry the clear potential for future expanded surveillance. We therefore urge you to reject this request.

This request comes at a particularly troubling time following recent reports that the Federal Bureau of Information (FBI) issued a request for proposal seeking a vendor, like Flock Safety, that will allow the FBI access to ALPR data collected nationwide.<sup>1</sup> The request before the Town Council is also being considered at a time when many municipalities across the country, including jurisdictions in nearby Massachusetts, are terminating their contracts with Flock Safety.<sup>2</sup> More locally, both Warren and Portsmouth recently rejected a request from the Rhode Island State Police to install the cameras in their towns.<sup>3</sup> The Council can – and we believe should – follow the lead of those municipalities moving away from these technologies.

Our organization has substantive concerns about the technology of these cameras, but we are just as worried by the possibility that these surveillance systems are being implemented without the concurrent introduction of statutory safeguards and limitations for their use. While we have reviewed the draft policy from the police department, that policy is notably lacking in meaningful privacy protections, and also could be amended at any time, without public input. Our major concerns with more context are as follows:

- **The cameras capture more information than just license plate numbers.** ALPRs are often portrayed as law enforcement tools that merely capture photographs of license plates. However, this framing minimizes the actual strength of these cameras. In reality, ALPRs can reveal a lot about a person. When combined, the data generated by these systems can reveal remarkably personal details

---

<sup>1</sup> <https://www.newsweek.com/fbi-plan-license-plate-data-track-drivers-nationwide-11967352>

<sup>2</sup> See, <https://www.cambridgema.gov/news/2025/12/statementontheflocksafetyalprcontracttermination>.

<sup>3</sup> To correct the record from the April 23 meeting, we would note that the Rhode Island State Police ALPR program required municipality approval for DOT permitting purposes.

about individuals' lives, like where a person attends religious services, where they work, where they sleep at night, what doctors they see, or where their children attend school.

Rhode Island's use of other ALPR systems – such as those utilized for tolling purposes or to enforce traffic violations – have generally been contained to capturing only the license plate on a vehicle, and only for a specific, narrow purpose. With Flock Safety ALPRs, as noted by Chief Raynes at the Council's April 23<sup>rd</sup> meeting, investigators may input a wide variety of vehicle characteristics into the system, which range far beyond license plates, including searches by vehicle type, make, color, license plate state, and other unique features like roof racks and even *bumper stickers*. 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 vehicle characteristics such as those noted above – and obtain information about a vehicle's whereabouts, when captured by a camera, for the preceding 30 days.<sup>4</sup> It is also worth noting that officers may input almost any reason when searching for a vehicle. We have seen numerous network and organizational audits that merely include vague references to “investigations” as reasons to search the system.<sup>5</sup> And further, these searches are not confined solely to a single jurisdiction. Search results can include images from an ALPR located in Little Compton, or any municipality participating in the nationwide sharing network, which includes camera systems located far outside Rhode Island.<sup>6</sup>

In fact, despite Chief Raynes' comments that federal immigration agencies “do not care about the back of a vehicle,” recent reports have revealed that Customs and Border Protection has conducted searches of Flock Safety's ALPR databases across the country to enforce the Trump Administration's anti-immigrant agenda.<sup>7</sup> At the same time, police departments have reportedly performed Flock Safety lookups on behalf of Immigration and Customs Enforcement (ICE), which does not have its own access.<sup>8</sup> Because of this data sharing model, any agency with access to Rhode Island's cameras could potentially share that information with other law enforcement agencies around the country. The nationwide misuses of this system do not stop there. Notably, this system has been utilized by police in other states to monitor protests, and also has been used by individual police officers to track former romantic partners.<sup>9</sup> In another disturbing use of the cameras, a police department in Texas used Flock

---

<sup>4</sup> Generally, Rhode Island jurisdictions that use ALPRs require data to be deleted after 30 days. This timeframe varies from state to state based on statutory limits. For example, Maine retains ALPR data for 21 days and New Hampshire requires the information to be deleted after three minutes. See <https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes>.

<sup>5</sup> A network audit is a list of all document searches of an agency's data conducted by outside users. An organizational audit is a list of internal searches of both the agency's data and the data of other agencies. <https://data.aclum.org/2025/10/07/flock-gives-law-enforcement-all-over-the-country-access-to-your-location/>

<sup>6</sup> For example, Woonsocket, RI shares camera data with dozens of municipalities including Houston, TX. See <https://transparency.flocksafety.com/woonsocket-ri-pd>

<sup>7</sup> <https://www.404media.co/cbp-had-access-to-more-than-80-000-flock-ai-cameras-nationwide/>

<sup>8</sup> <https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/>

<sup>9</sup> See, e.g., <https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists>; <https://wisconsinexaminer.com/2026/03/13/wisconsin-communities-grapple-with-police-misuse-of-flock-surveillance/>

Safety’s nationwide network to search more than 83,000 ALPR cameras to locate a woman suspected of having an abortion.<sup>10</sup>

• **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.** As the Council notably mentioned, there are no laws governing these systems in the State of Rhode Island. No matter what assurances of privacy are given in policy – by either a police department or Flock Safety – there are no meaningful constraints on either of their ability to change the rules at any time.<sup>11</sup> Today we may be told, for example, that all photos will be destroyed after 30 days, but nothing prevents the law enforcement agencies, or the company, six months from now from extending retention to 60 days, a year, or even a decade. The same is true for any other “safeguards” offered exclusively by police departmental policy or Flock Safety guidelines.

Since the Council is presently discussing the contractual terms of conditions, it is worth noting some recent and significant changes Flock Safety has made to their contracts that directly impact a municipality’s control over their data. Prior versions of Flock Safety’s terms and conditions explicitly stated that “Flock does not own and shall not sell Customer Data,” but that assurance has since been removed.<sup>12</sup> Instead, the newest version now grants the company “the exclusive right to determine and control the method, timing, format, and medium” of access to the data that allegedly belongs to the customer. The new terms and conditions now also give the company a “perpetual”<sup>13</sup> right to use the customer’s data to “support and improve” its services, effectively meaning that the company can use and retain footage forever – even after the customer has ended their contract with Flock, which is much longer than the 30-day retention period that is currently the standard in Rhode Island.<sup>14</sup>

The new contract terms also change the governing law from the state in which the customer is located to the State of Georgia, where Flock Safety is headquartered. Finally, and perhaps most relevant for the Council, the new contract provisions make it more difficult for customers to terminate contracts, and requires payment of services through the date of termination, regardless of which party terminates the agreement.<sup>15</sup>

• **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 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

---

<sup>10</sup> This is the scenario that Chief Raynes was alluding to in Texas regarding the potential searches of the system. <https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/>

<sup>11</sup> Legislation intended to regulate the use and procurement of these systems has been introduced in the past legislative sessions and have been held for further study in committee after facing opposition from law enforcement agencies. This year’s legislation includes new, explicit data sharing protections. See 2026-H 8077: <https://webserver.rilegislature.gov/BillText/BillText26/HouseText26/H8077.pdf>.

<sup>12</sup> <https://www.flocksafety.com/legal/terms-and-conditions>

<sup>13</sup> Section 4: “Data Use and Licensing,” of the contract before the Council.

<sup>14</sup> These changes are present in the contract the Council is discussing, and would apply to Little Compton ALPR data.

<sup>15</sup> <https://www.aclu.org/news/privacy-technology/flocks-terms-and-conditions>; Section 7 “Term and Termination,” of the contract before the Council.

does this gradually erode our expectations of privacy, but it also normalizes these surveillance progressions.

Even if not being used in more expansive ways today, the potential capabilities of an ALPR are not as narrow as simply identifying and cross-checking license plate numbers, and nothing prevents expanded uses in the future. The potential chilling effects on daily life as a result of the ability to track individuals in these manners cannot be overstated.

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 potential for inaccuracies of the NCIC database and the problems that alone can cause, it is clear now that these systems are not as narrowly tailored as residents may expect. Concerns about overreach are only compounded by the acknowledgement of the expansive surveillance properties contained in, and the invasive measures allowed by, these technologies.

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<sup>16</sup> 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.<sup>17</sup>

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 result of indiscriminate 24/7 surveillance. We know that public safety objectives can be met without sacrificing basic privacy protections or allowing unchecked 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.

For all these reasons, we urge the Town Council to reject the request to install a Flock Safety camera in Little Compton. The proposed policy does not provide adequate safeguards to protect the privacy rights of the Town and the States' residents. We would be happy to explain these issues in more detail or answer questions. Thank you for your consideration of these concerns.

Sincerely,



Madalyn McGunagle  
Policy Associate

cc: Scott Raynes, Chief of Police  
Anya Rader Wallack, Interim Town Administrator

<sup>16</sup> Transparency portals are online portals created by Flock Safety to show the public certain metrics in the use of these systems.

<sup>17</sup> <https://transparency.flocksafety.com/cranston-ri-pd>