



Bristol Police Department

395 METACOM AVENUE ◇ BRISTOL, RHODE ISLAND 02809
TELEPHONE (401) 253-6900



KEVIN M. LYNCH
Chief of Police

Flock Camera Program

Chief Kevin M. Lynch comments to the Honorable Bristol Town council

First, it has been an honor to be the Towns Chief of Police for the past seven years and lead an exceptional and ethical group of police officers. As you know, the department is both nationally and state accredited through CALEA and RIPAC and adheres to the highest ethical and professional policy standards. My submission will hopefully address some of the formal and informal concerns from concerned citizens regarding Automated License Plate Readers ("ALPR") a.k.a. Flock and address the safeguards that will be implemented to ensure compliance with federal, state, and local laws to include privacy issues.

Background: On Wednesday, November 12, 2025, the Rhode Island State Police ("RISP") sought approval from the Bristol Town Council at a scheduled and noticed meeting to install a Flock camera in the Town of Bristol on Metacom Avenue/Old Ferry Road in the vicinity of RWU/Mt. Hope Bridge. This program would provide access to the Bristol Police Department on a limited basis as a criminal investigative tool. Notably, the RISP (Captain Marc Alboum) provided verbal testimony on the program and their desire to partner with the Bristol Police Department with the Flock program at no cost to the Town *via* a grant received by the RISP. At the meeting the issue of sharing data was raised, and testimony was provided that the RISP will not be sharing any Flock camera data with federal law enforcement, more specifically, ICE as it relates to administrative immigration enforcement. Ultimately, the matter was tabled pending the RISP providing a formal written directive (General Order a.k.a. policy and Procedure) regarding their moratorium on sharing data with ICE.

Issues:

Will the RISP or BPD or even Flock share data with Ice or federal agencies involved in administrative immigration enforcement?

A - No, Flock does not have a contract with U.S. Immigration and Customs Enforcement (ICE) or any sub-agencies of the Department of Homeland Security. Flock does not share customer data with any federal agency.

Every piece of data collected by Flock license plate readers is owned and controlled by the local customer, whether that customer is a city, county, school district, or private organization. Agencies can share camera access with other police departments on a 1:1 basis, meaning one police department to another police department, by geographic radius (e.g., 10 miles), or statewide.

Note: RISP and BPD by written policy (General Order) depicts that they will NOT share any data with federal law enforcement (e.g., ICE) involved in administrative immigration enforcement.

Lastly, The Town Council and Bristol Police Department (“BPD”) has resolutions and policies that prohibits the police department from participating in civil immigration enforcement. (see attached)

Can ICE access Flock cameras on their own?

A - ICE cannot directly access Flock cameras or data. ICE does not have a master login, a hidden pathway, or a centralized feed into Flock systems. [Federal agencies](#), including ICE, cannot “tap into” Flock networks or independently search license plate reader data.

Has Flock Ever Had a Data Breach?

A - No, Flock Safety’s cloud platform has never experienced a data breach, and no [customer data](#) has ever been compromised. Flock technology includes Multi-Factor Authentication (MFA) by default and encourages all users to adopt MFA or Single Sign-On (SSO). Additional MFA methods are planned for rollout in 2026 to further strengthen account security. Flock does not maintain a centralized database of license plate reader data across customers. From the beginning, Flock was designed around the core principle that customers own and control their data. That design choice significantly reduces systemic risk.

Will Flock, RISP or BPD sell the data?

A - No such database exists. Customers own 100% of their data. Flock does not sell it. Only customers (police, neighborhoods, or businesses) decide who to share data with. Data is deleted after the retention period.

[Flock Safety](#) explicitly states they do not sell customer data; customers own their data, and Flock will never share or sell it to third parties, only the customer determines who accesses it.

How long will RISP or BPD store Flock data?

A - Flock’s standard retention period is thirty (30) calendar days from the date of capture. This standard retention period applies to all customer data, unless otherwise specified in the individual customer’s agreement. Data from Flock Safety devices is stored and then deleted after 30 days for privacy and security purposes. All images and metadata are encrypted throughout its entire lifecycle, from on-device to storage in the cloud. Flock uses Amazon Web Services cloud storage and KMS-based encryption, limiting access to the encryption keys. All CJIS data is stored in the AWS GovCloud and is only available to law enforcement agencies. No CJIS data is shared with non-Law Enforcement Flock Safety Customers.

What happens if the current technology or policy changes or advances?

A - Listed below in this submission is a visual aid to display the depth that ALPR (Flock Camera) can view an automobile license plate to include the rear of the vehicle. I suggest that any councilor that has concern(s) over advancement in technology or change in the current program or policy make their vote of approval contingent upon the current program and policies presented and any change to the policy or program will require a subsequent council approval.

Bristol is the safest community in RI. Why sacrifice our rights and support Flock?

A - Yes, even communities with low crime rates should invest in public safety, as these investments serve to prevent crime from happening in the first place, maintain the quality of life, sustain economic vitality, and address the root causes of potential future issues. Public safety is not just about responding to crime but proactively building a safe environment. *A reputation for safety attracts businesses and residents, which improves business vitality, increases civic participation, and helps property values rise.*

Is there legislation in RI governing the utilization of ALPR (Flock)?

A - Rhode Island currently lacks comprehensive statewide legislation for Automated License Plate Reader (ALPR) systems like [Flock cameras](#). While attempts have been made (like [H 7507](#) in 2022) to create state-level rules for data retention, sharing, and usage, these bills haven't fully passed, leaving communities to set their own guidelines. The RIPCA has longed supported legislation to establish similar guidelines that are already embedded in our policy and procedures in communities utilizing ALPR's (Flock). **Note:** Police departments operate every day in the country on General Orders, Policy and Procedures, MOU's and MOA's that govern their professional conduct and utilization on hundreds of important issues (e.g., Use of Force).

Does flock have Built-In Privacy Protections?

A - Flock's [license plate readers](#) ([LPRs](#)) are intentionally limited in scope:

- LPRs do not capture point-in-time images of vehicles on public roadways
- LPRs do not track vehicles continuously
- LPRs do not use facial recognition
- LPRs cannot search for personal traits such as race or gender
- LPRs do not collect personally identifiable information like names, addresses, or DMV records
- Images that are not used in an investigation are automatically deleted. The standard retention is 30 days unless a customer requires otherwise in accordance with local law or policy.

Can't the data be searched by anyone?

A - No. The Bristol Police Department is not participating in any sharing portal if granted access by the RISP.

Note: The ALPR program if approved will always be managed by a command staff member of the BPD. Additionally, the Bristol Police Department has robust policies to ensure compliance and protect civil liberties. Any violation of the policies could lead to employee discipline.

Link to Flock Safety – Separating Fact from Fiction – Security Claims and Facts:

<https://www.flocksafety.com/privacy-ethics>

Providence Journal Article – Dated February 12, 2022

Link: [Prying eyes? Surveillance cameras are making inroads in RI](#)

Is the Goal to Track People as the ACLU claims – Listed below is Colonel Michael Winkvist of the Rhode Island Police Chiefs Association response?

A - "We're not tracking people," said Col. Michael J. Winkvist, the police chief in Cranston, one of the first Rhode Island communities to use the Flock system. "All it does is give us a lead."

"I've been doing this for 31 years. This ranks toward the top of what I've seen," said Winkvist. "This is a great investigative tool. This is like having 29 officers sitting on various corners 24/7."

Winkvist said it can't invade anyone's privacy. "When you're on a public roadway," he said, "there's no expectation of privacy."

How is the system designed to work?

A - When a vehicle passes a camera, the system takes a still photo — not video — of the rear of the car. It then enters the date, time and location into a database, along with the license plate number and the vehicle's "fingerprint" color, make, bumper stickers, accessories such as bike racks and other details. Information can be used in two ways:

- If the car is wanted — the system has access to the National Crime Information Center database — the system will almost immediately alert the police where the car was spotted.
- The police can search for cars thought to be involved in crimes including hit-and-run crashes, missing people, civil and purple alerts, abductions, robberies and murders — by entering a description of the car and the time frame and geographic area where the vehicle would have been.



The Flock safety system only identifies a car license plate number, make and roof rack in this example from the company. Such information is entered into a database, along with the date, time and location of the photo, to help police investigations.

How the Flock system addresses privacy concerns?

Holly Beilin, a spokeswoman for Flock, said the system does not gather or record any information about who is driving a particular vehicle. The cameras, triggered by motion, capture still photos — not video — of the rear of a vehicle. "They're highly attuned to capture vehicles and license plates," Beilin said. "That is what they are made to do."

The system does not have facial recognition capabilities, she said.

"The cameras are focused on just the vehicle and the plate," Cranston's Colonel Winquist said.

"As far as racial profiling is concerned, it's the perfect system," Woonsocket's Chief Oates said, adding that the system knows nothing about the driver.

While the Flock system can read license plates and match those to wanted lists, it does not have access to registration information. Police departments have to manually run the plate to obtain that information.

Flock safety cameras helped crack the MIT and Brown Case

<https://www.boston.com/news/local-news/2025/12/19/flock-safety-cameras-helped-crack-the-mit-and-brown-case-but-at-what-cost-to-privacy/>

How Has Flock Safety Helped?

A - That information was simply a description of a vehicle: a gray Nissan. That one detail led police to search the network of more than 70 street cameras operated around the city by the technology company Flock Safety for video of the Nissan Sentra sedan with Florida plates. "That's how Flock was designed and built,"

said Josh Thomas, Chief Communications Officer of Flock Safety. “It was to help in exactly like situations like this.”

Investigators were able to access the Flock Safety system, enter the car’s description, and find a limited list of those in the area, Thomas said. Police narrowed it down further by searching for vehicles matching the description near Brown University. Since there was only one suspect car near Brown, the police used that license plate and entered it into the Flock system to see where else the cameras had picked up the plate in the last 30 days, crossing municipal and state borders.

Traditional license plate readers would not have been able to do this at all, let alone as efficiently. There was no initial license plate number to do a query. The software was able to go back in time, identify which cameras the car passed and when, and send a report to the officers.

By doing so, Thomas said, the police were able to connect the car back to the rental company.

“That’s how they got the lead that broke the case,” he said.



A Flock Safety camera spotted a gray Nissan Sentra with a Florida plate in Providence on Dec. 13. (Providence Police Department)

The tech firm that helped police find the Brown shooting suspect has sparked privacy concerns. Its CEO responds

<https://www.cnn.com/2025/12/19/tech/flock-safety-ai-cameras-brown-suspect-privacy>



*Flock Safety CEO Garrett Langley speaks at an event in Boston in July 2025. Flock's cameras were used to locate the suspected Brown University shooter in December 2025.
Danielle Parhizkaran/The Boston Globe/Getty Images*

New York —

On Thursday afternoon in New York City, I sat down with Flock Safety CEO Garrett Langley. We met to discuss the company's expansion from making cameras for reading license plates to building drones for law enforcement, and his response to recent privacy concerns surrounding Flock's technology.

Just hours later, Providence Police Chief Oscar Perez credited Flock's cameras and technology for helping to [locate](#) the Brown University shooting suspect.

To Langley, the situation underscored the value and importance of Flock's technology, despite mounting privacy concerns that have prompted some jurisdictions to cancel contracts with the company. "I think we run a risk today as a country that a generation of people will not believe America works for them because they don't feel safe, because in some communities ... you don't feel safe," Langley said. "It's too easy to get away with crime in America."

Finding the Brown shooting suspect?

Flock is a safety technology company that works with local law enforcement agencies and private companies. Its flagship product is an outdoor camera, referred to as "LPR" cameras, that can read license plates and identify other details about vehicles as they drive by. Flock's AI system allows police to search its network of footage for a specific car. Around 6,000 law enforcement agencies across the United States use its LPRs.

That's how Providence Police tracked down 48-year-old Claudio Neves Valente, who police say was responsible for both the Brown shooting and the killing of an MIT professor days later.

Perez described plugging a description of Valente's vehicle into Flock's system. One of Flock's cameras had recently spotted the car, helping police pinpoint Valente's location.

Responding to privacy concerns?

The company has faced criticism from some privacy advocates and community groups who worry that its networks of cameras are collecting too much personal information from private citizens and could be misused. Both the [Electronic Frontier Foundation](#) and the [American Civil Liberties Union](#) have urged communities not to work with Flock.

“State legislatures and local governments around the nation need to enact strong, meaningful protections of our privacy and way of life against this kind of AI surveillance machinery,” ACLU Senior Policy Analyst Jay Stanley wrote in an August blog [post](#).

“If (people are) worried about privacy, a license plate reader is the dumbest way to do surveillance. You have a cell phone. A cell phone knows your exact location at all times,” he said. “If you don’t trust law enforcement to do their job, that’s actually what you’re concerned about, and I’m not going to help people get over that.” Langley added that Flock has built some guardrails into its technology, including audit trails that show when data was accessed. He pointed to a [case in Georgia](#) where that audit found a police chief using data from LPR cameras to stalk and harass people. The chief resigned and was arrested and charged in November.

“We have to give law enforcement tools to do their job, and we should also hold them accountable to not break the law,” Langley said. “My whole philosophy as the CEO of Flock is: No one elected me president, no one elected me to be police chief of America,” Langley said. “It’s my job to build the tools and give the guardrails for how to implement them in different cities.”

Colonel Oscar Perez and Mayor Brett Smiley on Flock cameras:



<https://www.facebook.com/watch/?v=1350040883050555>

https://www.youtube.com/shorts/J_QxP0uo_Ws

Providence Police Chief, Col. Oscar Perez: **“Flock and the LPR was able to provide us with the description of this vehicle. ” The response to the Brown University and MIT shootings shows how speed, precision, and secure collaboration can drive results across jurisdictions”.**

Mayor Brett Smiley on flock?

A - Providence Mayor Brett Smiley supports [Flock license plate reader cameras](#), viewing them as essential technology for public safety and crime fighting, despite privacy concerns raised by groups like the ACLU; he emphasizes using them responsibly with safeguards for tracking illegal ATVs and solving serious crimes, integrating them with broader tech initiatives like the city's Real-Time Crime Center. Smiley backs these tools for enhancing officer capabilities, balancing safety with civil liberties, and addressing issues like illegal dirt bike use, though implementation details and privacy debates continue.



Chief Perez and Mayor Smiley say the new center is a win for public safety. Credit: Ian Donniss / The Public's Radio

Case Law – Supreme Judicial Court Findings (Massachusetts)

Commonwealth v. McCarthy (Massachusetts) is a key case on [Automated License Plate Readers](#) (ALPRs), where the Supreme Judicial Court (SJC) ruled that the Barnstable Police's warrantless, limited **ALPR data search didn't violate the Fourth Amendment**, but signaled that extensive ALPR data collection or searching could become a Fourth Amendment "search," requiring warrants, as it creates detailed movement histories akin to pervasive surveillance. **The SJC emphasized that while simple observation isn't a search**, aggregating large amounts of location data, especially historically, can reveal private details and trigger privacy protections.

Key Takeaways:

- **Limited Use vs. Extensive Data:** The court distinguished between a single plate scan (not a search) and mass data collection (potentially a search).
- **Reasonable Expectation of Privacy:** **The SJC found no reasonable expectation of privacy in the limited data in this specific case** but warned that widespread historical data could create one.

In essence, *McCarthy* set the stage for defining constitutional boundaries around evolving police surveillance technology, balancing law enforcement needs with individual privacy rights.

Conclusion:

I mentioned in my introduction I remain humbled and honored to be your Chief of Police, and I hope I have delivered both desired outcomes and results on all matters of public safety impacting the Town of Bristol – I must mention and appreciate the support from all of Bristol’s elected officials and department heads as without their support our goals for Bristol’s public safety would never have been met. Notably, the backbone of any success I have achieved has been the support obtained/mentioned and the hard and honest work of the men and women of the Bristol Police Department both sworn and civilian.

As you know, I lead the agency with integrity, vision, compassion and empathy for others and if the Flock camera program (ALPR) is approved by the Town council I pledge to ensure the strictest guidelines, reviews and accountability possible to safeguard our residents’ concerns regarding privacy issues.

Lastly, I remain hopeful that this tutorial will assist you in making a decision about Bristol’s future regarding public safety.

Yours in safety,

e-signature *Kevin M. Lynch*

Kevin M. Lynch
Chief of Police