

2026 JAN 23 AM 10:19

January 22, 2026

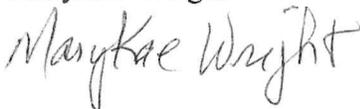
Dear Town Council members,

We are members of a group from Stand Up RI who have been very concerned about the dangers of adding the Flock surveillance system in our community. As a result, we have been delving deeply into the research about these cameras since November and would like to share with you a limited selection of the voluminous amount of information we have discovered, some of which we sent you earlier. Please see the attached articles.

We are hoping to speak at the Council meeting on the 28<sup>th</sup>.

Sincerely,

Suzanne Cohn  
Nancy Hood  
Nancy Kellner  
Annie Silvia  
Sharon Wollschlager  
Warren Wollschlager  
MaryKae Wright



## FLOCK LIABILITY CONCERNS - Prepared by Stand Up RI

The following summarizes our concerns related to the impact of Flock surveillance on individual privacy and civil rights and corresponding concerns related to municipal and individual liabilities. We have provided links to a few referenced or background articles and to the December 9, 2025, Warren Town Council meeting at the end of this document.

There is a lot of debate about weighing the safety benefits of Automatic License Plate Readers (ALPRs) like FLOCK against the negative impact of Flock surveillance on individual rights and personal freedom. The first link on page 2 (1) is a recent letter to the editor in the Bristol Phoenix explaining our opposition to the proposed rollout of FLOCK in Bristol as informed by the actual invasion on our personal privacy versus little if any empirical evidence regarding the benefit to our personal safety.

There is considerably less attention being paid to another significant factor when considering the installation and use of FLOCK cameras in our community, the real and potential legal and financial liabilities incurred by a municipality (and by extension its residents) when utilizing ALPR technology absent any Federal or State specific legislative and regulatory framework. There is a large and growing set of data documenting widespread and systematic abuse of Flock technology and data by individuals and governmental organizations and a growing body of information about potential legal risks associated with this abuse. These examples highlight the key risks and liabilities associated with Flock cameras for the Town of Bristol, and, by extension, for all of us residing in this town.

For instance, a pending federal lawsuit in Virginia alleges that Flock camera use is unconstitutional, that it constitutes a warrantless surveillance program in violation of the Fourth Amendment. (2) A motion to dismiss the lawsuit was denied, and this is an ongoing case. Privacy concerns are also heightened by the possible impact of the RI Data Transparency and Privacy Protection Act, effective January 1, 2026. There are any number of documented instances of Flock data being shared by agencies for unauthorized purposes such as immigration enforcement. A recent publication by the University of Washington Center documents numerous instances of unauthorized data sharing for purposes of tracking individuals and population groups. (3)

In addition to liabilities associated with privacy and civil rights, the Town of Bristol will face liabilities related to Flock data storage in the areas of data retention, security and misuse. Oregon Senator Ron Wyden recently requested the FTC investigate FLOCK for its failure to adequately protect data while needlessly exposing Americans' personal data to theft by hackers, foreign spies, and criminals. (4) We just experienced the hacking of Rhode Island's health exchange where the health data and social security numbers of hundreds of thousands of Rhode Island residents were compromised. (5) And just last month we learned that scammers gained access to Bristol's computers and stole more than \$300,000. (6) A superficial internet search identifies numerous examples of misuse of FLOCK data for personal reasons or unauthorized data access by officers or staff. (7)(8). Although Bristol will not control the FLOCK data, liability for data retention, storage and misuse is an open question. The Flock database is subject to hacking, just like any other database, and unfortunately we've all experienced the negative impact of data hacking and abuse right here in Bristol and throughout Rhode Island.

Another unresolved liability issue for Bristol (or any municipality) is the extent to which Flock data is or will be considered public and thus covered by the Public Records Act. A judge in the State of Washington recently ruled that Flock data is public. (9) This issue has not yet been litigated in Rhode Island, but a similar ruling in Rhode Island would mean that Flock data from Bristol would be subject to public records requests and litigation discovery with all the associated impact on financial and personnel resources.

The evidence that FLOCK cameras will significantly reduce violent or property crime in a small community like Bristol is anecdotal at best while the documented examples of problems with FLOCK data storage, access, and misuse are abundant. Not surprisingly, municipalities from Oregon to Massachusetts are either rejecting or cancelling their agreements with FLOCK. (10) We are seeing similar outcomes here in the East Bay where Newport recently postponed decisions about Flock and just last month the Warren Town Council rejected an identical Flock proposal from the RI State Police. During the December 9, 2025 meeting of the Warren Town Council, the Town Solicitor and Council members raised concerns about potential town liabilities in the absence of any regulatory framework. (11) In response the RI State Police indicated that they will be writing a policy to govern the use of these cameras and data. However, once the policy is written RISP will be able to change that policy or expand the capabilities of the cameras at any time. Importantly, in the absence of any applicable federal, state or local regulatory scheme, any proposed or actual contractual promises or agreements are basically unenforceable and every RI municipality faces significant liability should it choose to install a Flock camera.

These liability concerns are nonpartisan and have led conservative states such as Arkansas, Idaho and Montana to join Illinois, New York, Massachusetts and others to enact laws designed to protect the personal data collected through license plate readers and other means. Bristol should reject any Flock proposals absent critical regulatory safeguards designed to protect the State, its municipalities and every Rhode Island resident. Considering the significant impact on our personal privacy, the limited likely improvement in our personal safety and the very real municipal and individual liabilities associated with the utilization of Flock technology in Bristol absent any applicable regulatory safeguards, we urge you and your colleagues to vote no on the proposal to install a Flock camera in town.

- (1). <https://www.eastbayri.com/stories/letter-bristol-doesnt-need-intrusive-flock-cameras,136126?>
- (2). <https://www.forbes.com/sites/larsdaniel/2024/10/22/warrantless-surveillance-federal-lawsuit-challenges-flock-safety-cameras/>
- (3). <https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open/>
- (4). <https://www.wyden.senate.gov/news/press-releases/wyden-krishnamoorthi-urge-ftc-to-investigate-surveillance-tech-company-on-negligently-handling-americans-personal-data>
- (5) <https://governor.ri.gov/press-releases/governor-mckee-issues-update-cybersecurity-breach-ribridges-system>
- (6) <https://www.wpri.com/news/local-news/east-bay/california-man-charged-with-scamming-town-of-bristol-businesses/#/questions/5294859>
- (7). <https://thegeorgiagazette.com/featured/former-echols-county-sheriffs-office-employee-charged-after-allegedly-using-flock-system-to-stalk-people-she-knew/>
- (8). [https://www.kake.com/home/sedgwick-police-chief-tracked-ex-girlfriend-164-times-using-license-plate-cams/article\\_21fdfdb5-5dc5-11ef-95c4-8be8baa3f10c.html](https://www.kake.com/home/sedgwick-police-chief-tracked-ex-girlfriend-164-times-using-license-plate-cams/article_21fdfdb5-5dc5-11ef-95c4-8be8baa3f10c.html)
- (9). <https://www.eff.org/deeplinks/2025/11/washington-court-rules-data-captured-flock-safety-cameras-are-public-records?language=it>

(10) <https://www.politico.com/news/2025/11/30/license-plate-trackers-pushback-00670550>

(11). <https://www.youtube.com/watch?v=UqhF358ALnE> (RI State Police Presentation begins at about 17:45 mark) <https://www.eastbayri.com//////////stories/council-denies-state-police-request-to-install-flock-camera-in-warren,136195?newsletter=136255>

Prepared by StandUp RI – January 2026

**A critical consideration when discussing the use of Flock surveillance technology in Bristol should be the complete lack of any federal, state or local legal requirements or framework governing the use of Automatic License Plate Readers.**

1. FLOCK camera surveillance negatively impacts our individual freedoms, with little empirical evidence of reduction or elimination of crime in communities under 25,000.  
<https://www.eastbayri.com/stories/letter-bristol-doesnt-need-intrusive-flock-cameras.136126?>
2. There are potential liabilities for the Town of Bristol (and by extension its residents) associated with Flock camera surveillance including potential privacy and civil rights violations and unauthorized data sharing. <https://www.forbes.com/sites/larsdaniel/2024/10/22/warrantless-surveillance-federal-lawsuit-challenges-flock-safety-cameras/>; <https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open/>
3. Bristol could face liabilities associated with inadequate FLOCK data storage related to retention, security and misuse for unauthorized reasons. Flock surveillance constitutes a database, and databases get hacked. Just recently, we saw hundreds of thousands of people in RI face compromised identifying health data and social security numbers due to the hack of our health exchange, and Bristol reported theft of more than \$300,000 just last month after scammers accessed our databases. <https://governor.ri.gov/press-releases/governor-mckee-issues-update-cybersecurity-breach-ribridges-system> ; <https://www.wpri.com/news/local-news/east-bay/california-man-charged-with-scamming-town-of-bristol-businesses/#/questions/5294859>; <https://www.wyden.senate.gov/news/press-releases/wyden-krishnamoorthi-urge-ftc-to-investigate-surveillance-tech-company-on-negligently-handling-americans-personal-data>
4. Rhode Island Flock data might be determined to be covered under Public Records Act subject to freedom of information request and litigation discovery, as was the case in the State of Washington. <https://www.eff.org/deeplinks/2025/11/washington-court-rules-data-captured-flock-safety-cameras-are-public-records?language=it>
5. Additionally, municipalities have had to make financial settlements to residents falsely arrested or targeted due to Flock data errors. <https://www.nytimes.com/2024/02/05/us/aurora-family-police-settlement.html>

**Municipal liability for Bristol (and all towns in Rhode Island) is only heightened by the total absence of any federal, state or local statutes, regulations or regulatory schema addressing Automatic License Plate Readers. Liability concerns are nonpartisan and have led conservative states such as Arkansas, Idaho and Montana to join Illinois, New York Massachusetts and others to enact laws designed to protect the personal data collected through license plate readers and other means. Bristol should reject any Flock proposals absent critical regulatory safeguards designed to protect the State, all municipalities and every Rhode Island resident.**

Flock Uses Overseas Gig Workers to Build its Surveillance AI  
Joseph Cox  
404 Media

<https://www.404media.co/flock-uses-overseas-gig-workers-to-build-its-surveillance-ai/>

Dec 1, 2025 at 9:00 AM

Flock accidentally exposed training materials and a panel which tracked what its AI annotators were working on. It showed that Flock, which has cameras in thousands of U.S. communities, is using workers in the Philippines to review and classify footage.

This article was produced with support from WIRED.

Flock, the automatic license plate reader (ALPR) and AI-powered camera company, uses overseas workers from Upwork to train its machine learning algorithms, with training material telling workers how to review and categorize footage including images people and vehicles in the U.S., according to material reviewed by 404 Media that was accidentally exposed by the company.

The findings bring up questions about who exactly has access to footage collected by Flock surveillance cameras and where people reviewing the footage may be based. Flock has become a pervasive technology in the U.S., with its cameras present in thousands of communities that cops use everyday to investigate things like car jackings. Local police have also performed numerous lookups for ICE in the system.

Companies that use AI or machine learning regularly turn to overseas workers to train their algorithms, often because the labor is cheaper than hiring domestically. But the nature of Flock's business—creating a surveillance system that constantly monitors U.S. residents' movements—means that footage might be more sensitive than other AI training jobs.

Flock's cameras continuously scan the license plate, color, brand, and model of all vehicles that drive by. Law enforcement are then able to search cameras nationwide to see where else a vehicle has driven. Authorities typically dig through this data without a warrant, leading the American Civil Liberties Union (ACLU) and Electronic Frontier Foundation (EFF) to recently sue a city blanketed in nearly 500 Flock cameras.

Broadly, Flock uses AI or machine learning to automatically detect license plates, vehicles, and people, including what clothes they are wearing, from camera footage. A Flock patent also mentions cameras detecting "race."

## Flock haters cross political divides to remove error-prone cameras

Lawmakers' calls for Flock probe may help kill local contracts, expert says.

<https://arstechnica.com/tech-policy/2025/11/flock-haters-cross-political-divides-to-remove-error-prone-cameras/>

Ashley Belanger, Senior Policy Reporter – Nov 5, 2025 11:45 AM | [Arstechnica.com](https://arstechnica.com)

Ashley is a senior policy reporter for Ars Technica, dedicated to tracking social impacts of emerging policies and new technologies. She is a Chicago-based journalist with 20 years of experience.

Flock Safety—the surveillance company behind the country's largest network of automated license plate readers (ALPRs)—currently faces attacks on multiple fronts seeking to tear down the invasive and error-prone cameras across the US.

This week, two lawmakers, Sen. Ron Wyden (D-Ore.) and Rep. Raja Krishnamoorthi (D-Ill.), called for a federal investigation, alleging that Flock has been “negligently handling Americans’ personal data” by failing to use cybersecurity best practices. The month prior, Wyden wrote a letter to Flock CEO Garrett Langley, alleging that Flock’s security failures mean that “abuse of Flock cameras is inevitable” and that they threaten to expose billions of people’s harvested data should a catastrophic breach occur.

“In my view, local elected officials can best protect their constituents from the inevitable abuses of Flock cameras by removing Flock from their communities,” Wyden wrote.

Several communities have already come to this conclusion, although their concerns go beyond fears of hackers or potential data breaches.

They’re also concerned that law enforcement will use the sweeping database for invasive tracking. For instance, Texas scanned more than 80,000 ALPRs to allegedly do a wellness check on a woman suspected of self-administering an abortion, 404 Media reported.

Immigration and Customs Enforcement (ICE) has also worked with local police to conduct “immigration”-related searches of Flock data, 404 Media reported. (Langley wrote in a blog that providing ICE access is a local decision, “not Flock’s decision.”)

Reaching across the political spectrum, people in seven states have won fights to remove Flock’s invasive cameras in their towns and cities, sharing templates for success that are inspiring even more opposition campaigns. These critics oppose Flock not only because cameras threaten to violate the privacy of anyone who drives past them but also because the cameras are error-prone and can lead to wrongful detentions, the Electronic Frontier Foundation (EFF) reported.

For years, the EFF has tracked cases where ALPRs misread license plates, with the software accidentally reading an “H” as an “M” or a “2” as a “7.” Other times, ALPRs confuse the state on the license plate, giving cops the completely wrong target. Several Americans have been

accused of stealing cars because of these errors, some held at gunpoint and detained until the cops figured out the errors, the EFF reported.

And now, as Flock seeks to roll out a new product that would detect human threats by audio, there is another emerging threat widening the range of possible errors: police mishandling correct data. As cops nationwide increasingly come to rely too heavily on ALPR camera feeds, disturbing cases suggest that departments big and small tend to avoid basic police work as a check on the tech, which would prevent baseless accusations.

# Leaving the Door Wide Open: Flock Surveillance Systems Expose Washington Data to Immigration Enforcement

OCTOBER 21, 2025

## Summary

- Flock Safety automated license plate reader (ALPR) networks have become increasingly common in Washington state.
- Records obtained by UWCHR researchers via public records requests reveal that at least eight Washington state law enforcement agencies enabled direct, 1:1 sharing of their networks with U.S. Border Patrol at some point during 2025; effectively opening the “front door” for searches potentially related to civil immigration enforcement activities.
- Flock audits reveal apparent “back door” access by U.S. Border Patrol to the networks of at least ten Washington police departments which did not explicitly authorize Border Patrol searches of their network data.
- Flock audits reveal limited cases of law enforcement agencies in Washington state conducting “side door” searches on behalf of federal immigration enforcement agencies, as well as numerous similar searches by other law enforcement agencies nationwide with access to Flock networks in Washington state.
- Discrepancies between Flock audits and other documentation make it impossible for independent researchers to determine the current scope of local organizations’ access and exposure to searches by other Flock users nationwide.