112

Outlook

RECEIVED AT MEETING

TOWN CLERK'S OFFICE
BRISTOL, RHODE ISLAND
2026 JAN 28 PM 1:53

My opposition to Flock Cameras

From Margaret Elise Richards <margaretelise@gmail.com>
Date Wed 1/28/2026 12:33 PM
To Aaron Ley <aaron.ley@gmail.com>; nathancalouro@gmail.com <nathancalouro@gmail.com>; sweeneyforcouncil@gmail.com <sweeneyforcouncil@gmail.com>; maryp02809@gmail.com <maryp02809@gmail.com>; mrtonyteixeira@yahoo.com <mrtonyteixeira@yahoo.com>
Cc Melissa Cordeiro <mcordeiro@bristolri.gov>

1 attachment (876 KB)
bristol_flock_letter_full.pdf;

Dear Members of the Bristol Town Council,
Please find attached my concerns about installation of Flock cameras in the Town of Bristol. My arguments focus on issues related to data governance (i.e. who owns and controls access to and use of data), as that is an area of my professional expertise. I also included comments specific to the Flock presentation given at last night's Portsmouth Town Council meeting and the egregious ways Flock misuses "data" to highlight its effectiveness.

My professional and personal conclusion is that the risks imposed by adding Flock cameras to our town (and anywhere else) far outweigh potential benefits. I strongly urge you vote NO to this partnership with RISP.

The attached is quite detailed but it begins with a brief Executive Summary.

I thank you for your attention and your service.

Sincerely,
Margaret Richards
15 Ambrose Drive, Bristol

EXECUTIVE SUMMARY

Re: Proposed Flock ALPR Installation in Bristol

As a Bristol resident with six years of experience in federal data governance at the US Agency for International Development, I urge the Town Council to **decline approval** of the proposed Flock automated license plate reader (ALPR) installation. While I acknowledge that ALPR systems can assist law enforcement, the governance framework is fundamentally inadequate to justify the risks to residents' privacy, civil liberties, and municipal autonomy.

Key Concerns from a Data Governance Perspective

1. Bristol Does Not Control the Data

- The MOU explicitly states data are "owned by the Rhode Island State Police" with access granted "at the sole discretion of the Rhode Island State Police"
- Local policies cannot bind state authorities or future administrators
- Rhode Island lacks comprehensive ALPR legislation, leaving protections dependent on revocable internal policies

2. Federal Funding Creates Unknown Obligations

- The RISP grant was funded by the US Department of Justice
- Terms of the federal grant have not been made publicly available
- Terms of the RISP contract with Flock Safety have not been made public
- Bristol's MOU is inherently subordinate to federal grant requirements

3. Immigration Enforcement Restrictions Contain Significant Loopholes

- The prohibition applies only to "federal civil immigration law" enforcement
- Criminal immigration enforcement is not explicitly prohibited
- "Legitimate law enforcement purposes" language is broad enough to accommodate future policy shifts or federal mandates

4. ALPR Data Are Highly Identifying

- License plates are persistent identifiers that enable reconstruction of movement patterns
- The "mosaic effect": data can be combined with DMV records, property databases, other police databases, and commercial data brokers to identify individuals, their home addresses, workplaces, and patterns of life
- The claim that ALPR data are not "personally identifiable" ignores modern data-linking capabilities and is patently false in all practical senses

5. Data Retention Extends Beyond 30 Days

- While Flock purges data after 30 days, RISP General Order 80G requires that "information identified as criminal in nature...will be collected and retained using printouts and screenshots"
- This creates permanent records outside the 30-day window
  Anyone with access to the data can take a photo of it and do whatever they choose with it

6. Oversight Is Inadequate

- Quarterly audits review only 10 random searches—statistically insignificant for a system generating thousands of queries
- Chief Lynch's own memo cites a Georgia police chief who used Flock to stalk and harass individuals; the audit trail detected but did not prevent the misconduct

7. "Success Stories" Lack Counterfactual Analysis

- At Portsmouth's Town Council meeting (1/27/2026), Flock presented correlational data without rigorous impact studies
- There is no evidence that crimes would not have been solved without Flock cameras
- If Flock is "crucial" for effective policing, this implies current policing is ineffective—a claim few, if any, in Bristol would support

Recommendation

A central pillar of sound data governance is straightforward: when data collection poses potential risks to the individuals from whom it is collected, the default should be not to collect it. These risks include not only misuse of the data themselves, but also vulnerabilities created when datasets are combined, and the chilling effects on civil liberties when individuals know their movements are being systematically tracked and retained.

Bristol is "the safest community in RI" (Chief Lynch). Installing this technology asks residents to accept significant and lasting privacy risks for marginal gains. **I urge the Council to decline approval** and, if ALPR technology warrants future consideration, to wait until Rhode Island enacts comprehensive statutory protections with clear, enforceable limits on data use, retention, sharing, and resident rights.

DETAILED ANALYSIS

Dear Members of the Bristol Town Council,

I am writing to share my perspective on the proposed installation and use of Flock automated license plate reader (ALPR) cameras in the Town of Bristol.

I am writing as both a Bristol resident and someone who spent six years working in the U.S. Agency for International Development's Office of the Chief Information Officer, where I provided expert support on data governance. In that role, I addressed exactly the kinds of questions raised by systems like ALPRs: who owns the data, who controls it, how it can be shared, what risks are involved, and what protections actually exist—not just in policy language, but in practice.

A central pillar of sound data governance is straightforward: when data collection poses potential risks to the individuals from whom it is collected, the default should be not to collect it. These risks include not only misuse of the data themselves, but also vulnerabilities created when datasets are combined, and the chilling effects on civil liberties when individuals know their movements are being systematically tracked and retained.

I want to be very clear at the outset: I do not dispute that ALPR systems, including Flock cameras, can assist law enforcement in solving crimes such as identifying stolen vehicles or missing persons. **The issue before the Council, as I see it, is not whether the technology can be useful, but whether the governance framework under which it would operate in Bristol is strong enough to justify the risks it introduces.**

After reviewing the State Police request, the Memorandum of Understanding (MOU), the Rhode Island State Police General Order 80G on ALPR use, the Bristol Police Department's internal guidelines, the ACLU letter, and the Chief Lynch's comments, and last night's Portsmouth Town Council Meeting, **I have significant concerns that the answer is no.**

1. Town Policy Cannot Override State Data Ownership and Authority or Federal Funding Requirements

A central argument made by proponents of the Flock installation is that Bristol "controls its data" and can limit use and sharing through local policy and written assurances. However, the MOU explicitly contradicts this claim, stating unambiguously that "all data collected from FLOCK ALPR cameras is owned by the Rhode Island State Police and remains the property of the Rhode Island State Police. Access is granted at the sole discretion of the Rhode Island State Police and may be revoked at any time with or without cause."

In data governance terms, ownership matters. When data are owned at a higher level of government, local policies are inherently subordinate. Even if Bristol adopts stricter rules for itself, those rules do not bind the State. The town would have little to no recourse if state-level policy, leadership, or legal interpretations change in the future.

This is not hypothetical. As Chief Lynch's own memo acknowledges, "Rhode Island currently lacks comprehensive statewide legislation for Automated License Plate Reader (ALPR) systems." While attempts have been made—such as 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."

In the absence of statutory protections, policy safeguards rely almost entirely on internal general orders and MOUs that can be revised, reinterpreted, or rescinded by future administrators without public input or Council approval.

2. Immigration Enforcement Restrictions Contain Significant Loopholes

Much has been made of language prohibiting data sharing with U.S. Immigration and Customs Enforcement (ICE). However, the actual restriction is far narrower than it appears. Both the MOU and the State Police General Order prohibit sharing only "when the purpose of that agency or request is the enforcement of potential violations of **federal civil immigration law**" (emphasis added).

This language contains a critical loophole: it only restricts sharing for civil immigration enforcement. Criminal immigration enforcement is not explicitly prohibited. Furthermore, RISP General Order 80G states that "ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes"—language broad enough to accommodate future policy shifts, interagency agreements, or federal mandates that fall outside the narrow civil immigration carve-out.

From a governance perspective, restrictions defined by what they don't cover are inherently weaker than affirmative prohibitions. When policies rely on semantic distinctions ("civil" vs. "criminal") rather than categorical bans, they create exploitable ambiguity.

Furthermore, the RISP grant was funded by a Federal Agency—the US Department of Justice. Ultimately, anything our MOU says about data are subservient to the terms of this grant which, to my knowledge, have not been made publicly available. I do not assume ill intent, but I have encountered many cases in which federal funding recipients (including long-standing recipients) were out of compliance with federal requirements regarding data ownership, sovereignty, privacy and/or reporting. The consequences range from penalties to dangerous mishandling of data in efforts to comply with requirements after the fact.

3. The Data Collected Are Far More Revealing Than They Appear

It is repeatedly stated that Flock cameras do not collect "personally identifiable information." That framing is misleading. ALPR data are inherently identifying when viewed over time. License plates are persistent identifiers, and in fact the Rhode Island State Police General Order provides that license plates can be captured at private homes or businesses if viewable from a public road or place (which most homes are).

More importantly, ALPR data does not exist in isolation. It can be—and routinely is—combined with other publicly available or commercially available datasets to identify individuals, link vehicles to home addresses and home ownership, infer workplaces, medical visits, religious attendance, or political

activity. This is known as the "mosaic effect," and it is well recognized in both legal and data-governance contexts.

A license plate linked to timestamps and locations can easily be cross-referenced with DMV records, property databases, law enforcement databases or even commercially available data brokers to identify vehicle owners, their home addresses, work locations, and patterns of life. The assertion that ALPR data are not "personally identifiable" ignores modern data-linking capabilities.

No single dataset has to be invasive on its own to become invasive in practice.

4. Retrospective and Networked Surveillance Create Risks Beyond Bristol's Intent

ALPR systems enable retrospective searches: the ability to ask, weeks later, who was in a particular place at a particular time. While the data are purged after 30 days, that month-long window allows for extensive after-the-fact surveillance of people who are not suspected of any wrongdoing at the time of data collection. Examples of such data being used to identify protesters have been identified.

In addition, just because data are deleted from the Flock System does not ensure that they cannot be captured and maintained in other ways. In fact, Rhode Island State Police General Order 80G states that "Any information identified as criminal in nature that is obtained during an investigation from accessible **ALPR data will be collected and retained** using printouts and screenshots and shall be saved in the Evidence.com platform consistent with Records Retention Schedules."

When combined with regional or statewide sharing arrangements, this creates the capacity for broad, networked surveillance. The Rhode Island State Police General Order authorizes queries of "approved government or commercial databases with respective sharing agreements, memorandums of understanding, or intergovernmental agreements in place." Once Bristol's cameras are part of this network, the town participates in a surveillance infrastructure whose future scope it cannot fully dictate.

While current policies attempt to limit misuse, the architecture itself creates lasting capabilities that extend beyond any single administration's intentions.

5. Auditing and Accountability Mechanisms Are Insufficient

The State Police General Order requires quarterly audits consisting of "a random sampling of ten (10) browsing inquiries to ensure that each meets the requirements established by this policy."

For a system that could generate thousands of queries across multiple municipalities, auditing just 10 random searches per quarter is statistically insignificant. This represents a compliance-checking mechanism, not meaningful oversight. It provides the appearance of accountability without substantive protection against systematic misuse.

Moreover, even when misuse is detected, the consequences are unclear. Chief Lynch's own memo cites a case in Georgia where a police chief used Flock data to stalk and harass individuals. While Flock's audit trail ultimately caught the misconduct, it did not prevent it. The question for Bristol is not whether

violations can be detected after the fact, but whether we want to create the infrastructure that makes such violations possible in the first place. My own family member was stalked by a police officer ex-boyfriend using a police-issue GPS device. Warren Town Councilman Derrick Trombley has shared a similar story. In both cases ill intentions would only have been aided by Flock technoclogy.

6. Lack of Legislative Guardrails Increases, Rather Than Reduces, Risk

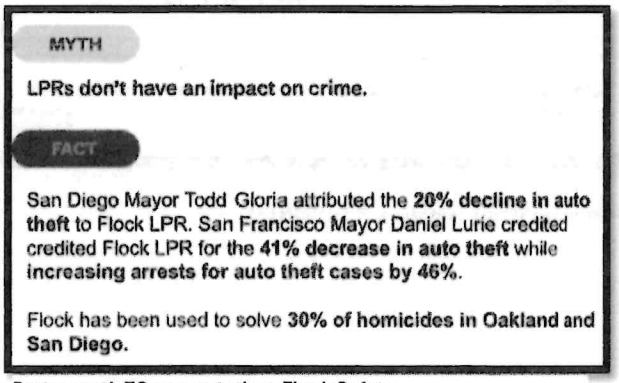
The Chief of Police correctly notes that "police departments operate every day in the country on General Orders, Policy and Procedures, MOU's and MOA's that govern their professional conduct." This is true. However, in the data-governance world, the absence of statutory guardrails increases risk; it does not mitigate it.

Internal policies provide guidance; statutes provide enforceable rights. Without clear state-level legislation governing retention periods, access controls, sharing restrictions, auditing requirements, and resident remedies for misuse, protections rely on institutional trust rather than legal accountability.

As someone who has worked on federal data policy, I can say candidly: trust is not a substitute for governance. Well-intentioned administrators retire. Political priorities shift. Budget pressures create incentives to monetize or share data in ways not originally contemplated. If Flock is as effective as its executives claim it to be I have little to no faith that they will not answer when Federal Agencies with deep pockets come knocking. Strong governance structures anticipate these realities and build in protections that outlast any individual actor's tenure.

Portsmouth Town Council Meeting – 1/27/2026

At last night's Portsmouth Town Council meeting, Flock representative Kerry McCormack shared a presentation that included "data" on impacts of Flock cameras in solving and preventing crime as well as a collage of headlines touting examples of how Flock has "impacted" the solving of crimes (quotation marks intentional).



Portsmouth TC presentation; Flock Safety

You may have heard the phrase "Correlation does not equal causation," which essentially means just because two things happened at the same time (i.e., Flock was used and a crime was solved) does NOT mean that one caused the other or that the other only happened BECAUSE of the presence of the first. In the absence of rigorous impact studies, there is no way to know that Flock was *responsible* for any of the crime statistics claimed by Flock.

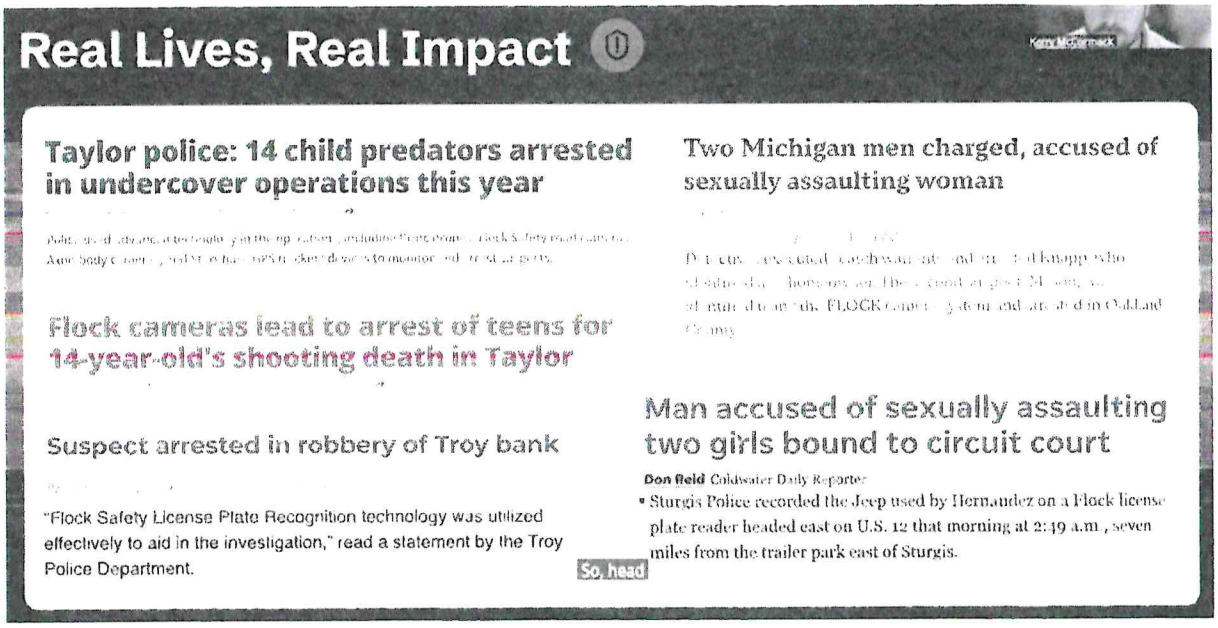
Also, the homicide statement is both ambiguous and irrelevant. Are we to assume that Flock was unable to "solve" 70% of homicides? Or that it was only used 30% of the time they were solved? More

importantly, there is no way to prove that in the absence of Flock these crimes would not have been solved anyway (i.e., that Flock cameras were material in solving them). Maybe the "best" cop was assigned to those 30% of cases. Maybe there were key witnesses in those 30% of cases.

The same logic applies to the Brown University shooting; just because Flock was used to find the shooter does not mean the shooter would not have been found without the camera.

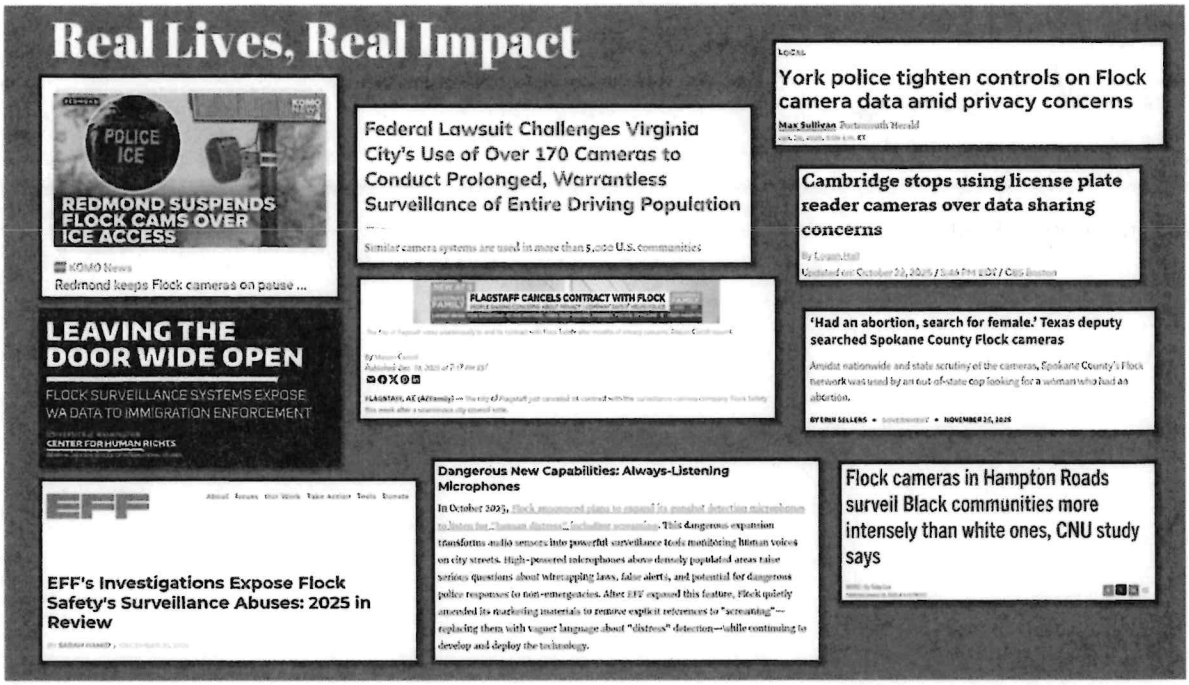
In a similar vein, if we are to assume that Flock cameras are crucial for effective policework, then what follows is that our current state is one characterized by "ineffective" policework. I don't think there are many in Bristol who would claim our police are ineffective (certainly not I). If that's the case, why assume all of these extra risks for little if any gain? I never heard of gains made by our last trial of similar technology.

As for the headlines,



Portsmouth TC presentation; Flock Safety 1

I compiled a list of my own.



Screenshots, Margaret Richards 1/28/26

Conclusion

Yes, Flock cameras can help catch criminals. The recent MIT and Brown University shooting case demonstrates this capability, though there is no way to construct a case-by-case counterfactual (would the case have been solved in the absence of Flock cameras?).

At the same time, that utility must be weighed against long-term risks—to privacy, civil liberties, public trust, and municipal autonomy—that are difficult to unwind once the infrastructure is in place.

The proposed safeguards are largely policy-based, subordinate to state AND federal authority, vulnerable to reinterpretation, and insufficient to counterbalance those risks. Bristol does not control the data. Bristol cannot bind future state administrators. Bristol cannot audit effectively at scale. And Bristol cannot prevent the mosaic effect once data enters a networked system.

As Chief Lynch himself notes, "Bristol is the safest community in RI." Installing a technology of this scope, under this governance framework, asks residents to accept significant and lasting exposure in exchange for marginal gains that could be pursued through less invasive means—including traditional investigative techniques, targeted camera deployment in high-crime areas, or support for legislative reforms that would establish real protections before infrastructure is deployed.

For these reasons, I respectfully urge the Town Council to decline approval of the proposed Flock ALPR installation at this time. If the Council believes ALPR technology merits consideration, I would encourage waiting until Rhode Island enacts comprehensive statutory protections that establish clear, enforceable limits on data use, retention, sharing, and resident rights.

Thank you for your careful consideration of this issue and for your service to the Town of Bristol.

Sincerely,

Margaret E. Richards

Margaret Richards

15 Ambrose Drive, Bristol