

[Your Full Name]

[[Your Street](#) Address]

[City, State, ZIP]

[Your Email Address]

[Your Phone Number]

[Date]

[County/City] Board of Commissioners (or City Council)

Attn: [Commissioner/Council Member Name(s),
or "All Commissioners/Council Members"]

[Government Building Name]

[Street Address]

[City, State, ZIP]

Sent via email to: [commissioner1@email.gov;
commissioner2@email.gov; ...]

RE: Urgent Request to Suspend and
Independently Audit the [Police Department
Name]'s Flock Safety ALPR Program

Dear [Chair/Mayor Name] and Members of the
[Board/Council Name],

I am a [County/City Name] resident writing to formally request that the [Board/Council] (1) immediately suspend further expansion of the [Police Department Name]'s ("[Department Abbreviation]") Flock Safety automated license plate reader ("ALPR") program, (2) commission an independent, public audit of how this system has actually been used, and (3) adopt binding policy safeguards before any further funds are committed to this vendor. I am raising this now because of a rapidly growing body of evidence — from across the country — showing that Flock Safety's audit and transparency systems, the very mechanisms local governments have relied on to reassure the public that this surveillance network is accountable, have been deliberately weakened at the same time misuse and abuse of these cameras is accelerating nationwide. [County/City Name] has invested in this system. [OPTIONAL: insert local contract details here —

total contract value, number of cameras, contract term, and funding source, if known. Example: "The County/City has approved a [X]-year, approximately \$[amount] contract with Flock Group Inc., operating [number] cameras as of [date]." Cite your local government's own press releases, council/commission meeting minutes, or budget documents.] Residents were told this network would be governed by transparent, auditable search logs. That premise is now in serious doubt.

Flock Safety Has Deliberately Gutted the Audit Logs That Were Supposed to Provide Accountability

In December 2025, Flock Safety unilaterally changed its Network Audit Logs so that they no longer include the officer's name, the specific license plate searched, the vehicle "fingerprint," or the open-text reason for a search — replacing this information with the word

"redacted." The company's own VP of Solutions stated this was done "to protect active investigations and ensure officer safety," but investigative reporting has shown this change followed public records requests that were successfully identifying individual officers' searches, and that Flock has told its own law enforcement customers it no longer trusts them with full information about who searched their own data (Footnote4a, "Flock Decides Cops Can't Be Trusted with Cop Data"). Separately, police departments have been explicitly instructed to be "as vague as permissible" when logging their reasons for searching Flock data, further degrading the usefulness of the one accountability tool the public has been told to rely on (Penn State Digital Shred, citing 404 Media reporting).

An audit log with the identity of the searcher blacked out is not an accountability tool. It is a

liability shield.

[OPTIONAL — add if applicable to your state: cite any local/regional misuse cases you have found via a public records request or local news coverage. Example structure: "In [Month/Year], [Agency Name] officers were [arrested/disciplined/terminated] after an internal or independent audit found they had misused Flock license plate data for [personal reasons / unauthorized purposes]." Search your state's news outlets and open records portal for department-specific findings before sending.]

Widespread, Confirmed Misuse Nationwide

This is not a hypothetical concern. Recent, independently reported cases include:

Five Albany, Georgia police officers were arrested and terminated after an internal audit found they misused Flock's retained license plate data for personal, non-law-enforcement purposes (USA Today).

[A Greene County, Georgia](#) sheriff's deputy and two supervisor-[level Cherokee County, Georgia](#) Sheriff's Office officers were separately arrested and terminated for accessing the Flock system for personal, non-investigative reasons (USA Today).

Atlanta News First Investigates identified at least 20 documented cases across Georgia in a single year of officers disciplined, fired, or criminally charged for misusing the Flock system, including allegations of tracking romantic partners and acquaintances (Atlanta News First).

The Electronic Frontier Foundation's analysis of more than 12 million logged searches by nearly 3,900 agencies nationwide found patterns of misuse targeting protesters exercising First Amendment rights and Romani people with discriminatory search terms, with no underlying criminal predicate (EFF, 2025 year in review).

If misuse of this scale is surfacing even under Flock's newly weakened audit standards, the [Board/Council] has no reasonable basis to assume [County/City]'s own deployment is exempt from the same risk.

Use of Flock Data for Immigration Enforcement, in Violation of Flock's Own Stated Policy

Flock Safety states publicly that it prohibits use of its data for civil immigration enforcement and that it has no contract with ICE (Flock Safety, "Does Flock Share Data With ICE?"). The evidence shows this prohibition is being routinely circumvented nationwide:

A Freedom of Information Act investigation by 404 Media found that ICE and Homeland Security Investigations have obtained "side-door" access to the Flock network by asking local and state law enforcement agencies to run searches on their behalf, despite having no formal contract with Flock — with more than

4,000 such lookups identified in a single analysis (Security Systems News; impolicytracking.org). The Electronic Frontier Foundation's June 2026 FOIA investigation found that Flock's own admin dashboard includes a drop-down menu allowing local police to subscribe their cameras to an ICE-controlled "Immigration Violator" hotlist populated entirely from civil administrative warrants that no judge ever reviewed — with at least two agencies confirmed to have enabled it, one of them in direct contradiction of its own written policy banning immigration enforcement use (TFTC, summarizing EFF findings). Dayton, Ohio found more than 7,100 immigration-related searches of its Flock data in explicit violation of its own policy, called them "egregious violations," and resorted to physically covering their cameras with trash bags because their vendor contract made it too difficult to

simply remove them (Fortune; Tech Times). Denver's redacted audit logs confirmed over 1,400 searches conducted on behalf of ICE despite the city's public assurances that no data was being shared with the agency (ACLU of Colorado); Virginia counties logged roughly 4,000 similar searches (VPM News); Washington state agencies were found to provide Border Patrol "front door," "back door," and "side door" access to Flock data (University of Washington Center for Human Rights); and by June 2026 at least 53 cities nationwide had cancelled their Flock contracts specifically over unauthorized federal data access (Tech Times).

Flock's leadership has been explicit that it will not enforce its own stated policy: CEO Garrett Langley has said compliance is left entirely up to local agencies and that Flock does not remove agencies from its network or cancel contracts over immigration-enforcement policy

violations (VPM News).

The Human Cost of Dragnet Surveillance and Aggressive Immigration Enforcement

This is not an abstract policy debate. In July 2026 alone, ICE agents fatally shot two people during operations in which federal officials themselves later admitted the person killed was not their intended target: Lorenzo Salgado Araujo, a 35-year U.S. resident, was shot and killed during a Houston traffic stop, with Homeland Security later confirming to a member of Congress that he was not the person being sought (AP News; The Independent Florida Alligator); and days later, a 26-year-old named Joan Sebastian Guerrero was shot and killed in Biddeford, Maine, in a case Senator Angus King's office says also involved a mistaken target (The New York Times; CBS News). A dragnet surveillance network that federal immigration agents can access

informally, without a contract, without a warrant, and without meaningful audit trail creates exactly the conditions in which these fatal, wrongful-target operations occur. Every additional Flock camera [County/City Name] installs is a potential input into that same apparatus.

Surveillance Without Evidence of Solving Crimes [County/City Name] has justified this spending on the promise of solving and deterring crime. The [Board/Council] should require [Department Abbreviation] to produce complete, current, independently verifiable statistics — not marketing figures supplied by Flock itself — on: the total number of ALPR searches conducted per year; the number of searches that led directly to an arrest, indictment, or conviction; and the number of searches for which no reason, or only a vague reason, was logged. Elsewhere, similar internal reviews have found

only a small fraction of searches are ever meaningfully audited (in one jurisdiction, exactly 10 searches were audited whether the annual total was 1,637 or over 10,000, The Morning Bun). Residents deserve the same rigor applied to our own program before another dollar is spent expanding it.

Requested Actions

I respectfully request that the [Board/Council]:
Immediately pause any further expansion of the [Department Abbreviation] Flock Safety camera network pending the outcomes below.

Direct [Department Abbreviation] to produce, and the [County/City] to publicly release, complete and unredacted Organization and Network Audit Logs for the past 24 months (redacting only what is strictly required by [cite your state's public records / open records statute], including officer identity, search justification, and any instance in which data was

accessed by or shared with any federal immigration enforcement agency.

Commission an independent, third-party audit — not one conducted by Flock Safety itself or relying solely on Flock's self-reported "Audit Assistance" tool — to determine how many searches of [County/City]'s Flock data have been conducted on behalf of, or shared with, ICE, Homeland Security Investigations, Customs and Border Protection, or any entity whose primary purpose is civil immigration enforcement.

Adopt a binding written policy, enforceable by contract and by local ordinance, that explicitly and permanently prohibits [Department Abbreviation] from sharing Flock data with, or running searches on behalf of, any federal immigration enforcement agency, and that requires immediate public disclosure of any violation.

Confirm that [Department Abbreviation]'s Flock system has not enabled any NCIC "Immigration Violator" hotlist or comparable federal watchlist feature, and if it has, disable it immediately.

Require full, unredacted officer-level audit reporting as a non-negotiable term of any renewed or renegotiated Flock Safety contract, and instruct legal counsel to evaluate whether Flock's revised terms and conditions — including new limits on data ownership and new arbitration requirements — are still in the jurisdiction's interest (ACLU).

Hold a public hearing, with advance public notice, dedicated specifically to this issue before any further funds are appropriated for this program.

[County/City] taxpayers have already committed significant public funds to this system. We are entitled to know who is looking at our data, why, and whether it is being used against our own

neighbors in ways this [Board/Council] never authorized. I ask that this letter be entered into the public record and that I receive a written response addressing each of the requests above. Thank you for your time and your service to this community. I look forward to your response.

Respectfully,

[Your Full Name]

[Your Address]

[Your Phone Number / Email]

HOW TO USE THIS TEMPLATE

Replace every bracketed field ([County/City Name], [Department Abbreviation], [Board/Council], etc.) with your local details.

Look up your own board/council members' current names and email addresses on your county or city government's official website — do not guess or reuse outdated names.

Add local specifics wherever marked

[OPTIONAL]: your local Flock contract value, camera count, and any local misuse or ICE-sharing cases you can find via your state's open records law, local news, or FOIA requests to your own police department. Local specificity is what makes a letter persuasive — the national examples above establish the pattern, but commissioners respond most to evidence from their own jurisdiction.

Verify your own state's public records/open records statute name and citation before sending (referenced in Requested Action #2).

Confirm current facts before sending — deadlines, names, and figures in this letter reflect reporting as of July 2026 and should be re-verified for accuracy at the time of use.

Consider also submitting this letter (or a condensed version) as public comment at a board/council meeting, in addition to mailing or emailing it.

If you obtain your own jurisdiction's Flock audit logs via a public records request, consider referencing haveibeenflocked.com's guidance on reading and interpreting them.