

A Liberty Response to Flock and the Networked Camera State

The case against automated license plate reader networks is not theoretical. It is a public record of stalking, protest surveillance, defeated safeguards, documented vendor lies, and innocent people held at gunpoint. This article assembles that record — and draws the only conclusion it supports.

The Argument in One Sentence

The danger of a system that photographs, timestamps, and geolocates every passing vehicle and stores it in a searchable national database is not that it *might* be abused. The capability itself is the injury — and no policy, audit log, or oath can neutralize a capability once it exists. Every safeguard Flock has offered has now been defeated in the field, documented, and in several cases exposed as a lie told directly to elected officials. What follows is not speculation. It is the record.

A Tool for Stalkers with Badges

The most common documented abuse is the simplest: an officer with access uses a nationwide movement-tracking tool on someone they are personally fixated on. The Institute for Justice has identified **at least 22 cases** of officers using ALPRs to track romantic interests — partners, exes, strangers — most since 2024. A partial docket:

- **Joplin, Missouri** — one officer ran one woman's plate nearly **400 times**, roughly a quarter of the entire department's searches, logging "DWI" or "Warrants" with no case numbers.
- **Milwaukee, Wisconsin** — an officer tracked a romantic partner and the partner's ex roughly 180 times in two months. It surfaced only because the *victims* searched their own plates on HaveIBeenFlocked.com. Then the detective **assigned to investigate that misuse was caught misusing the system himself**, logging his searches as "test" and "training."
- **Braselton, Georgia** — the police chief resigned and was arrested after women seeking protective orders said he used Flock to follow them and sent them maps of their own movements.
- **Oak Ridge, Tennessee** — a former officer was indicted on 23 counts of official misconduct, 18 of them for personal use of Flock.
- The same pattern has surfaced in **Costa Mesa, California; Orange City, Florida; Riverside County, California; Shelby County, Tennessee; Pasadena, Texas; Kenosha and Menasha, Wisconsin; Matteson, Illinois;**

Gwinnett County, Georgia; and Sedgwick, Kansas (another chief) — and Georgia media now report a running series of officer arrests across the state.

Note who caught them: **victims and activists using public audit tools — almost never the vendor's safeguards or the departments themselves.** Only a few of the twenty-two cases were initially discovered through internal investigation.



Surveilling Protected Activity

This is not scattered misconduct; it is systematic. The Electronic Frontier Foundation obtained datasets covering **more than 12 million searches logged by more than 3,900 agencies** between December 2024 and October 2025, and found:

- **More than 50 federal, state, and local agencies ran hundreds of searches connected to protest activity** — the 50501 protests, the "Hands Off" protests, and the No Kings demonstrations in June and October. Nineteen agencies ran dozens of searches tied to No Kings alone.
- **Tulsa PD** logged at least 38 protest-related searches, including one tied to a rally supporting a pro-Palestinian activist. **Tempe PD** ran an "attempt to locate" not for a specific plate but for *any red vehicle on the road* near a protest. **San Bernardino County** searched a vehicle across 711 networks with the reason logged simply as "no king."
- **Spokane County, Washington** deputies ran repeated protest searches — in direct violation of the sheriff's own written policy that its systems "shall not be used based on First Amendment activities." The policy existed. The searches happened anyway. That is the entire controls debate in one sentence.
- Agencies targeted **specific activist organizations**: Delaware State Police queried the network nine times over an animal-rights group's civil-disobedience actions.
- Audit logs contain searches using **ethnic slurs against Romani people** — one Texas department ran the slur six times through Flock's "Convoy" feature, which flags vehicles traveling together, profiling an entire community with no crime specified.
- A Texas sheriff's deputy used the national lookup to search **more than 83,000 cameras across the country** hunting for a woman over a self-managed abortion — logging "had an abortion, search for female" as his reason — and prosecutors later weighed criminal charges against her.

Driving to a protest, a church, a rally, or a clinic is not probable cause. The record shows it is treated as one.

PROTEST IS NOT PROBABLE CAUSE

12M

searches in EFF's dataset, logged by 3,900+ agencies over ten months

50+

federal, state & local agencies ran protest-related searches: No Kings · 50501 · Hands Off

711

camera networks searched for one vehicle by San Bernardino County — the logged reason: "no king"

38+

protest searches by Tulsa PD alone; Tempe PD ran a dragnet for ANY red vehicle near a protest

SPOKANE COUNTY'S WRITTEN POLICY BANNED FIRST AMENDMENT SEARCHES. DEPUTIES RAN THEM ANYWAY.

Source: Electronic Frontier Foundation analysis of Flock audit logs, Dec 2024 — Oct 2025; 404 Media; RANGE Media (Spokane County). All searches quoted from official audit logs.

Safeguards That Fail on Contact

- **The "reason" field is theater.** After the abortion search became public, Flock announced a "Proactive Search Term Tool" to block impermissible searches. An ACLU of Massachusetts investigation found police defeat it by typing vague reasons like "investigation" or "susp." One Oregon department entered **"hehehe"** as its justification **20 times in a single month** — and the searches went through.

- **The audits are not read.** Institute for Justice attorney Rob Frommer: "The audit processes these ALPR companies put in place are simply not being used. They are rarely, if ever, looked at after the fact." Several states then exempt the logs from public-records laws — so no one *can* look.
- **The scale of unaudited access is staggering.** In **Mountain View, California**, a statewide-lookup setting was on for 29 of 30 cameras without the police department's knowledge; over one year, **more than 250 agencies with no data-sharing agreement ran roughly 600,000 searches** of the city's data. In **San Jose**, an EFF/ACLU lawsuit documents **3,965,519 warrantless searches of one city's plate database in a single year.**
- **The company is weakening the safeguards it advertises.** Flock has begun redacting officer names from audit logs — the very accountability mechanism it points to — making future misuse harder for the public to detect.

THE REASON FIELD IS THEATER

"hehehe"

typed 20 times in one month as an Oregon department's
official search justification — every search went through

600,000

searches of one city's data by 250+
agencies with no data-sharing
agreement (Mountain View, CA)

3,965,519

warrantless searches of San Jose's
plate database in a single year —
now the subject of an EFF/ACLU suit

"THE AUDIT PROCESSES ... ARE SIMPLY NOT BEING USED."

Sources: ACLU of Massachusetts (search-tool test); Institute for Justice, EFF & ACLU of
California (California car tags); Mountain View, CA city records.

— Institute for Justice attorney, on ALPR audit logs

A Vendor That Lies to Its Own Customers

The ACLU's July 2026 report documents a pattern of Flock misleading not just the public but **the governments that buy its product**:

- **Oshkosh, Wisconsin** — At an April city council meeting, Flock's chief information security officer told the council its system did not "create a pattern or heat map of an individual's movement." The council approved the contract that day. By the next morning the city learned this was false; Flock later admitted its system does produce a heat map of a vehicle's captured

locations for up to a month. Oshkosh revoked the contract **one day after approving it** — Deputy Mayor Joe Stephenson: "I don't know how this body can govern... if you lie to me." Flock's response was to call the falsehood "one small misconception."

- **Loveland, Colorado** — When the police chief asked whether federal agents were accessing town data, Flock said federal agencies no longer had access, and the CEO told the press Flock had no federal contracts. The company was later forced to admit it had pilot contracts giving federal agencies direct access to plate data. The CEO's explanation: "We clearly communicated poorly."
- **Fabricated endorsements** — Flock has repeatedly claimed to have "worked with" or "partnered with" the ACLU on system design and legislation. The ACLU's response: neither the national organization nor any affiliate has ever partnered with Flock on anything.
- **Attacking critics instead of fixing problems** — When security researchers found at least 70 cameras exposed to the open internet with no password (live footage of children in parks viewable by anyone), Flock's response was to smear researchers as activists who want to "defund the police" and "normalize lawlessness." When 404 Media published critical reporting, the company said the critics were "trying to let murderers go free." The CEO emailed all law-enforcement clients declaring that Flock was "under coordinated attack" — and characterized public-records requests, the basic machinery of democratic transparency, as a "weapon."

A company whose denials have repeatedly turned out to be false has forfeited the presumption of truth on every remaining claim — including its claim that misuse is rare.

The Contract Is a Trap

The ACLU's analysis of Flock's revised terms and conditions, changed in February 2026, found the company has:

- **Removed** the sentence "Flock does not own and shall not sell Customer Data" from its terms.
- Granted itself a **"perpetual" license** to use customer data to "support and improve" its services — meaning it keeps using a community's surveillance data **even after the city terminates the contract** and loses access itself.
- Kept "the exclusive right to determine and control the method, timing, format, and medium" of the customer's access to its *own* data — with reports that customers receive degraded, low-resolution copies stripped of metadata.
- Expanded its liability protections, mandated private arbitration under Georgia law, and made termination harder — including when a council votes the contract down or declines to fund it.

A city does not buy cameras from Flock. It surrenders its residents' movement history to a private corporation, in perpetuity, on terms the corporation rewrites at will.

When the Machine Is Right, It Still Ruins the Innocent

Set deliberate abuse aside entirely. By Flock's own figures its readers are roughly 93% accurate across roughly 20 billion scans a month — arithmetic that yields **on the order of a billion misreads every month**, any of which can appear on a squad-car screen as grounds for a felony stop. The Institute for Justice has documented **at least 26 cases since 2018** — most since 2023 — of innocent motorists pulled over, held at gunpoint, jailed, or attacked by police dogs over a misread or unverified alert:

- **Sherwood, Arkansas** — a couple held at gunpoint over a misread character while their six-week-old baby sat alone in the back seat.
- **Morristown, Tennessee** — an "O" read as "0"; grandparents at gunpoint while their three-year-old granddaughter watched.
- **Toledo, Ohio** — a "7" read as a "2"; the driver was mauled by a police dog and jailed.
- **San Diego, California** — a man spent nearly a month in jail over Thanksgiving after the system wrongly tied him to a carjacking five miles from where he actually was.
- **Colorado** — a woman summonsed for package theft on camera "evidence" had to assemble her own dashcam and a neighbor's doorbell footage to prove she was never there — the presumption of innocence run in reverse.
- **Plymouth, Minnesota** — an automotive journalist was boxed in by four squad cars after a dealership's plate typo propagated through the national network; officers told him they had been tracking him **for days**.
- **Canyon County, Idaho** — tort claims have been filed against the cities of Wilder and Caldwell alleging the systems violate civil rights. The liability is now arriving in court.

A BILLION MISTAKES EVERY MONTH

$$93\% \times 20B = 1B+$$

claimed accuracy scans / month misreads / month

26+

innocent motorists stopped, held at gunpoint, jailed, or attacked by a police dog over a misread or unverified alert (IJ, since 2018)

SHERWOOD, AR

couple at gunpoint; 6-week-old alone in the back seat

MORRISTOWN, TN

an '0' read as '0' — grandparents at gunpoint before a 3-year-old

TOLEDO, OH

a '7' read as a '2' — mauled by a police dog, then jailed

SAN DIEGO, CA

nearly a month in jail over Thanksgiving on a false match

PLYMOUTH, MN

boxed in by 4 squad cars over a dealership typo; tracked for days

EVERY MISREAD IS PROBABLE CAUSE ON SOMEBODY'S SCREEN.

Sources: Flock's published accuracy & scan volume; Institute for Justice (26+ wrongful-stop cases since 2018); local reporting: Sherwood AR, Morristown TN, Toledo OH, San Diego CA, Plymouth MN.

The Trajectory Is Always Expansion

Internal documents obtained by reporters describe a product ("Nova") designed to link plate data with commercial data brokers across some 20 data sources so police can "jump from LPR to person" — demolishing the company's long-standing claim that it collects no personally identifiable information. The company has announced video clips and live feeds from its cameras, natural-language AI search of everything the cameras see ("pickup truck with a ladder" — or anything else,

including people), drones, and cameras that track pedestrians rather than vehicles. Mass surveillance never stays the size it was sold at.

Why Controls Cannot Fix This

Each failure above defeats a specific safeguard that was supposed to prevent it. That is the point — the failures are not gaps in the design; they *are* the design.

- A **required reason field** that accepts "hehehe" twenty times restrains no one.
- An **audit log** no one reads — and that states shield from public-records law, and that the vendor now strips names from — is not accountability; it is a receipt issued after your stalker's 400th search.
- A **written policy** against First Amendment surveillance did not stop a single one of Spokane County's protest searches.
- A **local ordinance** binds only local officers, while 250 strange agencies run 600,000 searches through the back of the system.
- A **vendor's promise** is worth exactly what Oshkosh learned it was worth: one day.

Grant, generously, that every control were tightened. The capability remains: a standing, retrospective, searchable record of where ordinary people go, built by watching people who have done nothing wrong. You cannot audit that away. It is not a bug in the system. It is the system.

Meeting the Objections

"It solves crimes." Sometimes it does — recovered vehicles, missing persons, closed cases. That is real. But effectiveness is where the analysis begins, not where it ends: wiretapping every phone would also solve crimes. The question a free society asks is whether the price is a permanent architecture of suspicionless tracking, and whether narrower tools — targeted cameras that check plates against hot lists and flush non-hits, warrants, ordinary investigation — reach the same ends without cataloguing everyone.

"Misuse is rare — fewer than 15 cases among 140,000 users." That is the vendor's number, and it is contradicted by the public record it doesn't control: the Institute for Justice counts 22-plus stalking cases *alone*, before counting protest surveillance, slur-driven profiling, wrongful detentions, or unauthorized cross-agency access in the hundreds of thousands of searches. More fundamentally, the count only includes officers who were *caught* — overwhelmingly by victims and activists, not by the system. A denominator of undetected abuse is unknowable by design, and a company documented lying about its own capabilities cannot certify its own safety record.

"There's no expectation of privacy on public roads." That doctrine was built for isolated human observation, not persistent networked tracking of everyone. The Supreme Court recognized the difference in *Carpenter v. United States* (2018): comprehensive retrospective location records are categorically different from a glimpse, even when each data point is "public." The ACLU has now put that

argument before the Fourth Circuit as applied to ALPR networks, and litigation is multiplying — San Jose, the Idaho tort claims, and beyond. A thousand public moments, stitched together and stored, become a private life.

The Liberty Argument Proper

Strip away every incident above and the objection still stands. Even if no officer ever stalked an ex, no protester was ever logged, and no innocent man ever faced a drawn gun over a misread digit — a permanent, suspicionless record of the movements of a free people would still be intolerable. The right to drive to a lawyer, a doctor, a church, a gun store, a protest, or a lover without generating an entry in a police-searchable database is not a privilege the state extends when it promises to behave. It is a precondition of self-government.

Surveillance infrastructure does not ask permission to be abused; it waits. Governments change. Policies change. Access widens. The one constant is that a capability built today will be used to its limit by someone tomorrow — and the record above shows "tomorrow" arrived years ago. More than 55 communities have already terminated their contracts. They are not paranoid. They read the audit logs.

The right response is not a better reason field, a stricter policy, or a louder promise. It is to take the cameras down.

Sources

- **ACLU** — "Flock Lied About its ALPR Technology. What Else Has It Lied About?" (July 2026); "Municipalities: Beware of Changes in Flock's Legal Terms"; "Flock CEO Goes Ballistic on Critics"; "Flock's Aggressive Expansions"; the Get The Flock Out campaign and Fourth Circuit amicus brief.
- **Electronic Frontier Foundation** — "How Cops Are Using Flock Safety's ALPR Network to Surveil Protesters and Activists" (12-million-search dataset analysis); 2025 Year in Review (Romani slur searches, activist targeting, San Jose lawsuit).
- **Institute for Justice** — reports documenting 22+ officer-stalking cases and 26+ wrongful detentions from ALPR errors; attorney statements on unused audits.
- **404 Media** — officer-misuse reporting, exposed-camera security research, the "Nova" data-broker product, protest-monitoring data.
- **The Marshall Project; Business Insider; FOX6 Milwaukee; Wisconsin Examiner; Straight Arrow News; The Drive; Denverite; KTVB (Canyon County tort claims); Truthout; RANGE Media (Spokane)** — individual case reporting cited above.
- **HaveIBeenFlocked.com** — public audit-log search; tracks Flock contract-term changes.
- ***Carpenter v. United States***, 585 U.S. 296 (2018).

Every incident above is a matter of public record. Follow the sources; the record is worse than the summary.