



*Get
the
Flock
Out*

Evaluating and Regulating Automatic License Plate Readers (ALPRs) in the Context of Protecting Civil Rights & Civil Liberties

Chad Marlow, Senior Policy Counsel, ACLU

SEPTEMBER 10, 2026

ACLU

ACLU
Pennsylvania

Before we get started...*Spoiler Alert!*

Anti-surveillance bills, including those that regulate the use of Automatic License Plate Readers (ALPRs) are **NON-PARTISAN**



What are ALPRs and How Do They Operate?



- Digital cameras
- Stationary and mobile operation
- Capture and record:
 - License plate number + state
 - Vehicle location (including date and time)
 - Sometimes vehicle make, model, color, and even scratches and bumper stickers
- Can capture billions of plate scans every month

Analyzing Surveillance Technologies from a Civil Rights & Civil Liberties Perspective

Option 1

Too problematic to use
under any circumstances

Option 2

Risky, but safer to use in
limited contexts with the
right guardrails in place

Which bucket ALPRs fall into is your call to make...

3-Step Process for Considering ALPR Legislation

Step One

Do the benefits of using ALPRs ever exceed its risks to individual rights?

- If “no”, ban ALPR use.

Step Two

With respect to each potential ALPR use, do the benefits of that specific use exceed its risks?

- Where the answer is “no”, do not permit that use.

Step Three

If the benefits outweigh the risks to one or more potential ALPR uses, then:

- Determine what legal guardrails must be implemented to safeguard civil rights and liberties, including the right to privacy, from the risks the allowed ALPR uses presents.

A Note on Surveillance Decision Making

Just because a surveillance technology's use may be legally or constitutionally permissible doesn't mean, as a matter of public policy, that it is a good idea and must be allowed.



ALPR Threats to Civil Rights & Liberties

❖ Threats to privacy

- Location tracking
- Ability to remain anonymous in public
- Expectation of privacy in public
- Data sharing

❖ Discriminatory targeting/deployment

❖ Unjustified stops and false arrests

THE 4TH AMENDMENT
OF THE UNITED STATES CONSTITUTION 1791
THE RIGHT OF THE PEOPLE TO BE SECURE
IN THEIR PERSONS HOUSES PAPERS AND
AGAINST UNREASONABLE
SEARCHES AND SEIZURES
SHALL NOT BE VIOLATED
AND NO WARRANTS SHALL ISSUE
BUT UPON PROBABLE CAUSE
SUPPORTED BY OATH OR AFFIRMATION
AND PARTICULARLY DESCRIBING THE PLACE TO BE SEARCHED
AND THE PERSONS OR THINGS TO BE SEIZED

Specific ALPR Threats in 2026



ALPRs have been used by federal, state, and local agencies to identify and track:

- Immigrants (ICE)
- Protestors (50+ federal, state, and local agencies)
- Op-ed writers (local police)
- Gun show attendees (DEA/ATF)
- Abortion care seekers (state/local police)

ALPR Bans–Straightforward & Growing in Popularity

Florida

In August 2026, banned the use of ALPRs on all state highways.

Texas

In August 2026, halted all ALPR funding and paused installation of ALPRs statewide.

Vermont

Effective July 1, 2027, banned all government use of ALPRs.



ALPR Guardrail: Use Limitations

Problem

ALPRs can be used to target disfavored and vulnerable groups, for minor crime enforcement, and to generate suspicion out of thin air.

Solution

Limit use to only the worst crimes (e.g., kidnapping). Prohibit inappropriate uses (e.g., identifying protestors). Perhaps allow certain non-law enforcement uses (e.g., toll collection).



ALPR Guardrail: Data Retention

Problem

The more ALPR data that is captured and the longer it is retained, the more private information it reveals.

Solution

Significantly limit ALPR data retention to a few days unless linked to a specific investigation.



ALPR Guardrail: Data Retention (con't)

Problem

State law cannot protect against federal agency demands for state/local ALPR data made through a judicial warrant or administrative subpoena.

Solution

Significantly limit ALPR data retention. If you don't have the data, you cannot be forced to turn it over.



ALPR Guardrail: Data Sharing

Problem

Without data sharing limits, ALPR data can be made available to unknown and untrusted recipients.

Solution

Ideally, prohibit data sharing outside of collecting department unless requestor has a judicial warrant. Next best option—limit ALPR data sharing to only PA state and local entities, unless the requesting entity has a warrant for a crime recognized in PA.



ALPR Guardrail: Unreliable Databases

Problem

Not all criminal databases against which ALPR data is run are reliable. Some do not even comply with basic accuracy, reliability, and completeness requirements.

Solution

Limit the “hotlists” ALPR data can be run against to reliable, well-maintained state and local databases from Pennsylvania.



ALPR Guardrail: Discriminatory Deployment

Problem

It is not uncommon for ALPRs to be exclusively or disproportionately deployed against specific, vulnerable communities.

Solution

Require ALPR deployment to be equitable and uniform throughout a jurisdiction.



ALPR Guardrail: Local Rules Problem

Problem

When localities are tasked with establishing their own ALPR rules, civil rights and civil liberties protections will be uneven and can be inadequate.

Solution

State law should establish clear and consistent ALPR rules and guardrails.



(Worst) Case Study: Flock Safety

There are a lot of dangerous ALPR companies whose business models are based on trading people's privacy in return for massive profits.

The *worst* of them is Flock Safety.

In the past 18 months, more than **200** localities nationwide have ended their relationships with Flock, including an average of **3.5 terminations per day** in August 2026.



Flock Problem: Data Retention

After insisting for years that it needed to retain ALPR data for at least **30 days**, in August 2026 Flock reduced its default retention period to **7 days**.

But that is just a default.

If requested, Flock will retain ALPR data **only for as long is permitted by state and local law**.

Flock Problem: Data Sharing...With Anyone

According to Flock's "Government Agency Customer Agreement":

"Flock may access, use, preserve and/or **disclose the [ALPR] Footage to law enforcement authorities, government officials, and/or third parties** ... if Flock has a good faith belief that such use, access, preservation or disclosure is reasonably necessary to ... protect the rights, property, or safety of Flock, its users, a third party, or the public as required or permitted by law."

Flock Problem: Data Sharing...Anywhere

According to Flock's "Government Agency Customer Agreement":

"[The customer] Agency hereby grants Flock a non-exclusive, **worldwide, perpetual, royalty-free right** and license (during and after the Service Term hereof) to ... **disclose the Agency Data and Non-Agency End User Data (both inclusive of any Footage)** to enable law enforcement monitoring against law enforcement hot lists as well as provide Footage search access to law enforcement for investigative purposes only."

Flock Problem: Poor Data Security

CLAIM: Flock repeatedly makes misleading data security claims like: ***“Does Flock Share Data With ICE? No. Flock does not work with U.S. Immigration and Customs Enforcement (ICE) or any other sub-agency of the Department of Homeland Security. Flock does not partner with ICE. ICE does not have direct access to Flock cameras, systems, or data.”*** (January 6, 2026)

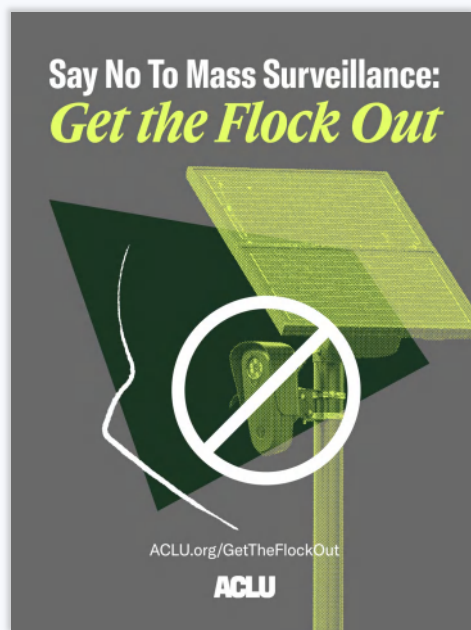
FLOCK’S REALITY:

- For years, ICE repeatedly accessed Flock’s data indirectly by asking authorized Flock customers to access it for them. In June 2026, Flock finally admitted ICE can access its data but claimed it’s “not our problem”.
- While Flock says its database search features are designed to prevent unauthorized and inappropriate searches, it accepts searches for almost any reason, including “investigation” and “Hehehe”.
- While Flock says its system is secure, Flock cameras and data have been hacked in minutes by investigative journalists.

Flock Problem: National ALPR System

Flock's stated corporate goal is to expand to “*every city in the United States,*” and to build a “*national camera network*” using local ALPRs and their data.

What's Next: #GetTheFlockOut of Pennsylvania



www.aclu.org/GTFO

But it's not just Flock. Beware of other ALPR companies like Axon and Motorola/Vigilant.

NEWS & COMMENTARY

Beware of Other License Plate Surveillance Companies Besides Flock

Flock deserves the heat it's getting, but switching to another provider won't necessarily improve anything



aclu.org/news/privacy-technology/other-alpr-vendors

ACLU

Contact Us

Chad Marlow

Senior Policy Counsel

ACLU

CMarlow@aclu.org

Liz Randol

Legislative Director

ACLU-PA

ERandol@aclupa.org

Veronica Miller

Deputy Legislative Director

ACLU-PA

VMiller@aclupa.org



ACTU