

The Data Can Be Right While the Outcome Can Be Dangerously Wrong—or Deadly

Arthur R. Leggett

Revised infographic-integrated blog draft | September 7, 2026

Automated license plate readers can help recover stolen vehicles, locate missing children and identify vehicles connected to serious crimes. Those are legitimate and sometimes lifesaving uses.

But the usefulness of ALPR technology should make us more careful about what it proves—not less.

Top 7 States

#	State	Cameras
1	California	20,197
2	Texas	16,524
3	Georgia	9,654
4	Florida	9,456
5	Illinois	7,138
6	Ohio	6,726
7	New York	4,221

Bottom 3 States

#	State	Cameras
1	Vermont	30
2	Hawaii	52
3	Montana	62

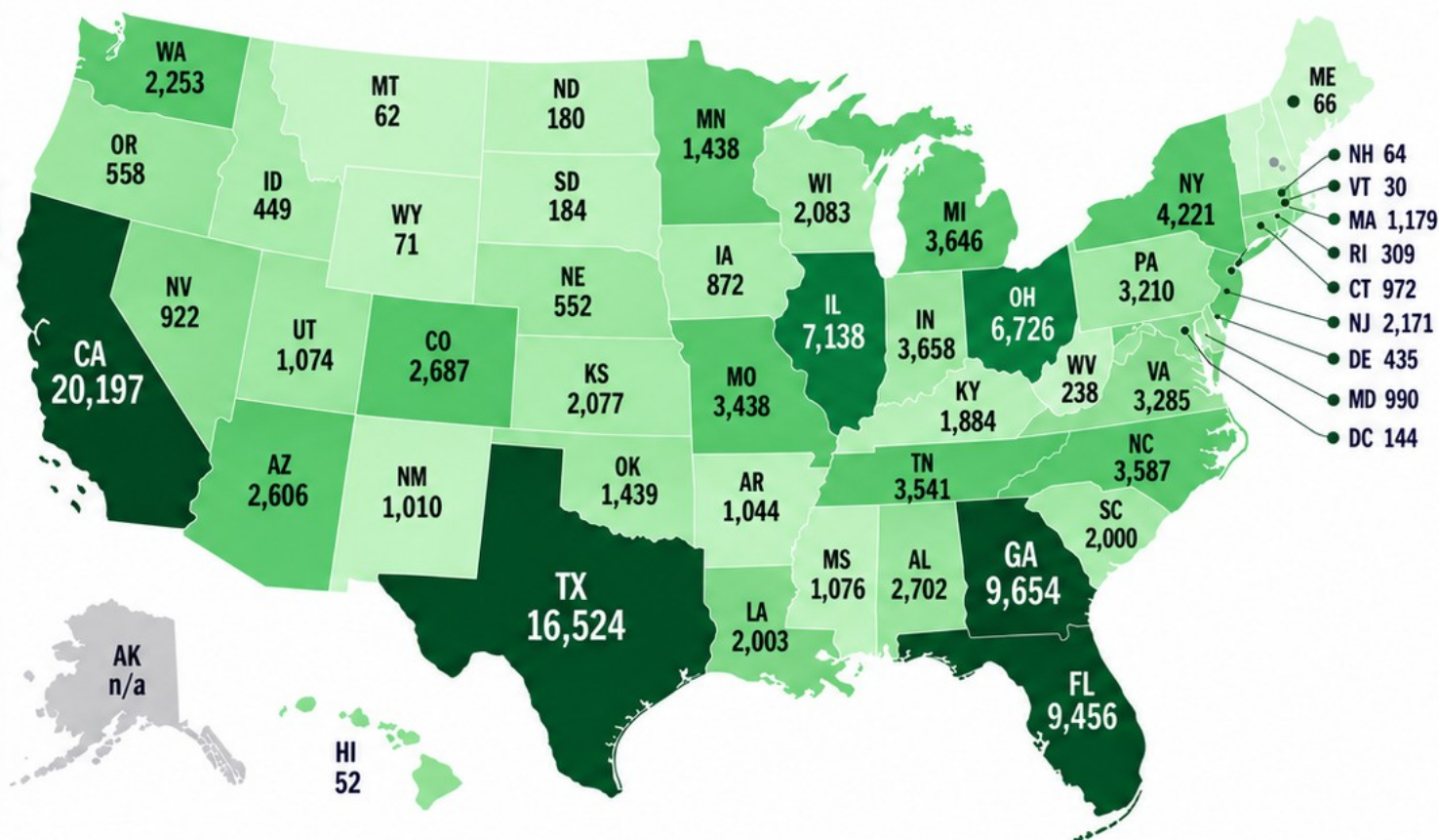
Cameras per state

10,001+
5,001 – 10,000
2,001 – 5,000
501 – 2,000
101 – 500
1 – 100
No data

Community-Reported ALPR Cameras Across the United States

At least 136,157 cameras are mapped across 49 states and Washington, D.C.

State counts reflect community-reported mapped cameras and may not include every installation. The map includes ALPRs from multiple manufacturers; about 77% are explicitly tagged as Flock Safety.



Note: Counts are community-reported mapped cameras from FlockCameraLocations.com (OpenStreetMap data), accessed Sept. 5, 2026.

Counts may be incomplete or out of date. Alaska had no count displayed on the source index page.

Source: FlockCameraLocations.com (OpenStreetMap, community-reported camera map).

— By Arthur Roark Leggett

A license-plate reader identifies a plate associated with a vehicle.

It does not identify the driver.

It does not establish who is riding in the vehicle.

It does not establish what those people are doing.

And it certainly does not establish criminal conduct.

Yet a plate can begin a consequential chain of reasoning:

```
license plate → registered owner → presumed driver → presumed occupants → presumed conduct
                                     → police action
```

Every arrow is an inference.

Every inference creates another opportunity for error.

And the plate is no longer necessarily the starting point.

Modern systems can also search by vehicle characteristics, using observable features to narrow the universe of possible vehicles when a plate is unknown, obscured or unreliable.

That creates another chain:

```
vehicle characteristics → candidate vehicle → associated person → presumed driver → presumed
                                     conduct → police action
```

Again, each step introduces an inference. That is what makes the technology powerful. It is also what makes it dangerous when investigators, institutions or automated systems begin treating an inference as a fact.

The system may correctly identify a vehicle.

The conclusion drawn from that identification can still be wrong.

Flock ALPR Cameras: Real Benefits. Real Risks.

Powerful tool for public safety — but not without serious tradeoffs.

Automated license plate readers (ALPRs) like Flock can help solve crimes and find missing people. But they also raise privacy, accuracy, and governance concerns that cities and states must address.

THE PROS

Public Safety, Efficiency, and Community Benefits



1

Helps Solve Serious Crimes

Has aided arrests in homicides, assaults, robberies, and car thefts.



2

Finds Missing and Exploited People

Helps locate missing children and human trafficking victims.



3

Recovers Stolen Vehicles

Helps identify and recover stolen cars quickly, often across state lines.



4

Improves Law Enforcement Efficiency

Provides real-time alerts, automates plate checks, and saves investigative time.



5

Supports Multi-Jurisdictional Cooperation

Helps agencies share information across city, state, and federal partners.



6

Produces Leads, Not Proof

ALPR hits are a starting point for investigation, not a conviction.



THE CONS

Privacy, Accuracy, and Governance Risks



1

Driver is Inferred, Not Proven

A license plate shows a vehicle, not who was driving — risking false assumptions.



2

Enables Historical Tracking

Mass collection can allow long-term movement histories and create surveillance risks without a warrant.



3

Data May Be Inaccurate

Misreads, outdated records, and stolen or shared plates can lead to false leads or wrongful stops.



4

Risk of Misuse and Overreach

Access by unauthorized users or for non-criminal purposes can erode trust and civil liberties.



5

Limited Transparency and Oversight

Policies, data retention, and audit practices often vary and are not always public.



6

Mission Creep

Tools built for serious crime can expand to broader enforcement, civil uses, or revenue-generating applications.



THE BOTTOM LINE

The policy challenge is not whether ALPRs can work. It is whether their benefits can be preserved without allowing bad data, misuse, and retrospective surveillance to outrun accountability.

Source: USA TODAY, "Frequent Flockers: Repeat searches prompt officer firings, arrests," Aug. 28, 2026; FlockCameraLocations.com, "Locations by state," OpenStreetMap community-reported data, accessed Sept. 5, 2026.
Note: Not all location counts are community-reported and may be incomplete or out of date; they are not an official Flock Safety inventory.

By Arthur Roark Leggett
Data can inform a safer tomorrow.

Consider dirty data.

Brian Hofer rented a Getaround vehicle for a Thanksgiving trip in 2018. The car had previously been reported stolen and later recovered. But according to allegations in a federal court filing, information available to the automated license-plate-reader system still treated the recovered rental car as stolen.

When an ALPR scanned the plate, Contra Costa County sheriff's deputies stopped the vehicle. Hofer and his brother alleged that deputies surrounded the car, drew weapons, handcuffed them and searched the vehicle before confirming that the rental was legitimate.

Consider what happened:

The plate was correctly read.

The camera performed as designed.

The vehicle had once been stolen.

But the information driving the alert no longer reflected the vehicle's actual status.

The technology did not have to malfunction for the encounter to become dangerous.

That distinction matters.

A database tells us what it contains. It does not tell us whether what it contains is still true. And once information moves among police departments, vendors and interconnected databases, correcting an error can become much harder than creating one.

Dirty data are only one vulnerability.

Another is deliberately poisoned data.

Someone seeking to harm another person may not need to hack an ALPR system. A malicious actor could instead manipulate the information that causes law enforcement to begin searching for a vehicle.

false report → vehicle association → ALPR hit → presumed conduct → police action

The camera can still perform perfectly.

The system can still locate exactly the vehicle it was told to locate.

The failure occurred before the search began.

The premise was false.

That should force law-enforcement agencies to distinguish between two very different questions:

TWO QUESTIONS

Did the system correctly find the vehicle?

Was there a legitimate and sufficiently verified reason to look for that vehicle in the first place?

Then there is authorized misuse.

This is not hypothetical.

Haines City police officer Christopher Goodson was arrested in August 2026 after investigators alleged that he searched the Flock license-plate database for his estranged wife's vehicle 717 times between September 2024 and June 2026. Investigators said the vehicle was not connected to a criminal investigation requiring those searches and alleged that differing law-enforcement justifications were entered for the queries.

That case exposes a different weakness.

The officer allegedly did not break into the system.

He had permission to use it.

That means the question cannot stop at: Who is authorized to search?

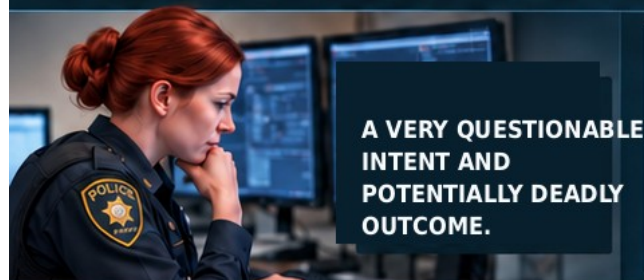
We must also ask what an authorized user must provide before conducting a search: a documented investigative purpose, a case number, reasonable suspicion, probable cause—and at some point, a warrant.

UNCHECKED ALPR ACCESS, **POTENTIAL RISKS**

HOW LEGITIMATE ACCESS CAN BECOME PERSONAL SURVEILLANCE — A SEVEN-DAY SCENARIO IN BUTTE, MONTANA

FICTIONAL SCENARIO BASED ON REAL RISKS
For training and awareness purposes only.

BUTTE
MONTANA
RICH HISTORY. REAL PEOPLE.



**A VERY QUESTIONABLE
INTENT AND
POTENTIALLY DEADLY
OUTCOME.**

EX-HUSBAND'S TRUCK



2019 Ford F-150
Montana Plate: 7A-3842K
Registered to: Ex-husband

WOMAN'S LEXUS SUV



2022 Lexus RX 350
Montana Plate: 4T-9931M
Registered to: J. Carter

ALL READS ARE ACCURATE.

Each ALPR detection correctly captured a real license plate, at a real time and location.

The system is working as designed.
The misuse is the problem.

DAY 1

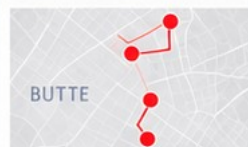
MON, APR 7

Officer searches:

Q 7A-3842K

ALPR hits:

8:22 AM Harrison Ave
12:06 PM Front St
5:41 PM Harrison Ave



● Ex-husband's truck

Officer runs her ex-husband's plate "to see if he's in town." Three legitimate reads.

DAY 2

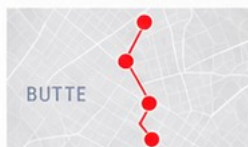
TUE, APR 8

Officer searches:

Q 7A-3842K
(multiple times)

ALPR hits:

7:55 AM Montana St
12:31 PM Uptown
6:18 PM Harrison Ave



Ex-husband's daily travel signature emerges.

DAY 3

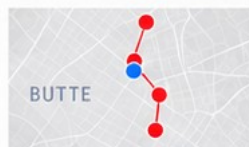
WED, APR 9

Officer searches:

Q 7A-3842K

ALPR hits:

8:03 AM Montana St
12:28 PM Uptown
5:52 PM Harrison Ave



● Ex-husband's truck
● White Lexus SUV

A white SUV is noticed meeting up with the ex-husband's pickup truck. The officer searches the plate 4T-9931M.

DAY 4

THU, APR 10

Officer searches:

Q 7A-3842K 7:12 AM
Q 4T-9931M 7:13 AM

ALPR hits:

8:01 AM Montana St
12:20 PM Uptown
6:05 PM Both vehicles at same location (2-minute window)



● Ex-husband's truck
● White Lexus SUV

Both vehicles are noticed again at the same location.

DAY 5

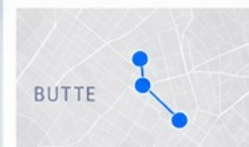
FRI, APR 11

Officer searches:

Q 4T-9931M
(multiple times)

ALPR hits (Lexus):

7:46 AM Women's Gym
11:52 AM Nail Bar
2:17 PM Hair Salon
6:04 PM Montana St



● White Lexus SUV

Focus shifts to the woman's Lexus. Officer tracks her day at a women's gym, a nail bar, and a hair salon, revealing her routine and personal activities.

DAY 6

SAT, APR 12

Officer searches:

Q 4T-9931M
(multiple times)

ALPR hits (Lexus):

8:11 AM Pilates Studio
10:24 AM Local Brunch
1:37 PM Trader Joe's
6:02 PM Montana St
7:14 PM Home (east side)



● White Lexus SUV

Officer continues to track the woman's routine, capturing a Pilates studio visit, brunch at a local spot, and grocery shopping at Trader Joe's, building a clearer picture of the target's weekly routines.

DAY 7

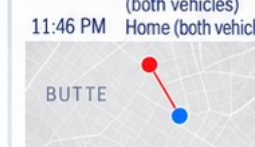
SUN, APR 13

Officer searches:

Q 7A-3842K
Q 4T-9931M
(multiple times)

ALPR hits (both vehicles):

1:12 AM Ex-husband's home (both vehicles)
9:03 AM Hiking Trail (both vehicles)
12:17 PM Busy Lunch Spot (both vehicles)
11:46 PM Home (both vehicles)



● Ex-husband's truck
● White Lexus SUV

Both vehicles are seen at the ex-husband's home overnight. The officer tracks them to a popular hiking trail and to a busy lunch spot, then back to the ex-husband's place where she lurks outside the bedroom window with her firearm drawn.



THE DATA CAN BE MISUSED AND ABUSED.

Accurate reads can be used to stalk, monitor, and surveil innocent people.

THE DATA CAN LEAD TO REVEALING INFERENCES.

Data can reveal route or driving signatures and unannounced relationships.



THE ACCESS ENABLES THE ABUSE.

The officer did not hack the system. She had legitimate access — and used it for a personal vendetta unrelated to any criminal investigation.



THE AGGREGATION CREATES A LIFE MAP.

A week of accurate reads can reveal patterns, routines and sensitive locations, effectively reconstructing a person's life.



THE RISK IS REAL.

Nothing in this scenario required the technology to fail. The danger comes from intent, access, aggregation and the absence of effective safeguards.

**THE SAME TOOL THAT HELPS SOLVE CRIMES CAN ALSO BE USED TO TRACK INNOCENT PEOPLE.
SAFEGUARDS ARE NOT OPTIONAL — THEY ARE ESSENTIAL.**

**ACCURATE DATA.
GREATER RESPONSIBILITY.
A SAFER TOMORROW.**

SCENARIO TAKEAWAY

The data can be used to stalk, monitor, and surveil the innocent.

Day 7 refinement: after the pair return from a hiking trail and lunch, the officer waits outside the ex-husband's home with her 9mm drawn.

WHEN LOCATION CAN BECOME A WEAPON

The ability to locate and follow another person can become especially dangerous when jealousy, obsession and access to a firearm enter the equation.

Location-based stalking can escalate from monitoring, to fixation, to confrontation—and violence.

BEHAVIORAL CONTEXT — NOT AN ALPR CASE

In a 2011 Meridian, Idaho, case later featured on Dateline, Rob Hall went to a Walgreens after learning that his wife, Kandi, was there with her lover, Emmett Corrigan. The confrontation ended with Hall shooting Corrigan dead. The relevance to the fictional Butte scenario is behavioral, not technological: location knowledge can become especially dangerous when jealousy, obsession and access to a firearm converge.

Source: Dateline NBC, "Deadly Desire." This was not an ALPR case.

Those questions become more important as ALPR changes from a real-time investigative tool into a system capable of reconstructing a person's movements.

A real-time alert that a stolen vehicle just passed a camera is one thing.

A historical search that reveals where someone routinely goes, when they tend to go there and how those locations connect is something fundamentally different.

Enough observations can reveal patterns.

Patterns can reveal routines.

And routines can begin to reveal a life.

That is the point at which an investigative tool starts to resemble surveillance.

Nashville's ALPR rules already incorporate part of that distinction. Metro Nashville Police policy requires reasonable suspicion involving specified offenses before authorized employees examine ALPR information collected more than one hour earlier. The department also restricts access, logs and audits searches, and requires two levels of verification of a fixed-camera hit before officers are authorized to conduct a vehicle stop.

Those safeguards matter. But they lead to a larger question:

WHEN DOES AN INVESTIGATIVE SEARCH BECOME SURVEILLANCE?

The law has not supplied a simple answer for ALPR.

In March 2026, the Fifth Circuit held in *United States v. Porter* that an ALPR alert identifying a vehicle associated with a person wanted on an outstanding arrest warrant, combined with the information available to the officer, supplied reasonable suspicion for the traffic stop that followed.

That was a limited investigative use. Location information becomes constitutionally more complicated as its depth and scope increase.

In June 2026, the Supreme Court held in *Chatrie v. United States* that government acquisition of Google's Location History data constituted a Fourth Amendment search because individuals have a reasonable expectation of privacy in their cellphone location information.

The case involved cellphone data, not ALPR, and therefore does not settle the license-plate question.

But it reinforces an important principle: technological observations can become qualitatively different when the government gains the ability to reconstruct where a person has been.

A single observation tells law enforcement where a vehicle was. A large collection of observations can reveal where a person worships, works, sleeps, seeks medical care, spends the night, visits family or meets another person.

At sufficient scale, location data stop functioning as isolated observations.

They become a map of someone's life.

That suggests a reasonable hierarchy of safeguards.

A real-time ALPR hit should require verification.

A retrospective database search should require a documented investigative justification and case number.

A search intended to reconstruct a person's historical movements should require judicial authorization absent a genuine emergency.

That is not hostility toward law enforcement.

It is skepticism proportional to power.

Flock itself announced stronger controls in August 2026, including broader case-code requirements, automated misuse detection and mechanisms to suspend access when user behavior meets defined criteria for abnormal activity pending review.

But another risk emerges once the infrastructure is established: mission expansion.

A network originally justified by stolen cars, missing children and violent crime can also be used for parking enforcement, tolls, registrations, fines and other administrative purposes.

That expansion is not theoretical. In 2026, Albany, California, sought ALPR equipment for parking enforcement, including technology capable of identifying vehicles with outstanding parking violations in real time.

Parking enforcement is lawful.

That is not the point.

The point is that the incentive structure changes.

public-safety tool → broader enforcement tool → revenue-producing platform

Once a system can generate revenue, policymakers should ask a question that does not arise when the sole purpose is finding an abducted child:

DOES THE INCENTIVE CHANGE?

Does the institution operating the system now have a financial incentive to expand its use?

Technology rarely remains confined to its first application. Once the infrastructure exists, additional uses become easier to justify.

So the central question is not merely: Can we do this?

It is: What should we permit the system to do?

What should a search require?

Who verifies the underlying data?

Who audits authorized users?

How are errors corrected across police departments, vendors and interconnected systems?

When should a judge have to approve a search?

And who is accountable when a technically accurate system helps produce a dangerously inaccurate outcome?

ALPRs can be valuable crime-fighting tools. They can help solve crimes. They can detect stolen vehicles. They can save lives.

None of those benefits require us to suspend skepticism.

Quite the opposite.

The more efficiently technology converts data into law-enforcement action, the more carefully we should examine every inference between the two.

Because the camera can be right.

The plate can be right.

The database can return exactly what it contains.

The software can operate exactly as designed.

And the conclusion can still be wrong.

Dangerously wrong.

Or deadly.

Arthur R. Leggett