



Power Demands Accountability

*A SAFE Framework for Automated License Plate Readers
and Government Surveillance*

NO. 001 • POLICY PAPER • JULY 2026

“The public should not have to choose between a useful investigative tool and a free society. We should design the system to deliver both.”



Publication note. This paper is a policy proposal, not legal advice. It uses automated license plate readers as the immediate case study, but its principles are intended for government use of automated public-surveillance technology more broadly. Laws and cases were reviewed through July 29, 2026.

Executive Summary

Automated license plate readers, or ALPRs, can do real good. They can help locate an abducted child, recover a stolen vehicle, identify a car connected to a violent crime, and sometimes confirm that an innocent person was nowhere near the scene. Those are not hypothetical benefits, and a serious privacy proposal should not pretend otherwise.

The danger is not the camera by itself. The danger is the combination of scale, retention, networking, analytics, and unilateral access. A person driving on a public road can be seen by anyone nearby. That does not automatically mean government should be able to build a searchable history of where that person traveled, who traveled with them, which homes or businesses they visited, and what patterns can be inferred from those movements - all without a warrant, meaningful approval, or later notice.

That is the line this paper addresses.

I am not arguing that ALPR systems should disappear. Law enforcement operated before these systems existed, and it would continue to operate without them. But ALPR technology can materially improve legitimate investigations, so the better question is not whether the tool is all good or all bad. The better question is: **What standards must a system this powerful meet before the public should trust it?**

My answer is the SAFE Framework:

- **Specificity:** Every search should be tied to a lawful purpose and be no broader than necessary.
- **Authorization:** Approval should scale with the breadth, sensitivity, and number of people affected by a request.
- **Freedom:** Privacy, association, due process, and the presumption of innocence should be protected by default.
- **Enforcement:** The rules should be public, technically enforced, independently audited, and backed by real remedies.

The framework rests on one governing principle: **trust but verify**. A legitimate investigator should be able to use the tool. No single investigator should be able to misuse it in secret.

The central recommendations are straightforward:

1. Establish a federal minimum floor while preserving stronger state and local protections.
2. Require every jurisdiction to publish its own ALPR policy before deployment.
3. Use proportional authorization, with at least two-person approval for non-warrant exploratory searches and higher approval for broad or intrusive requests. This is not a suggestion that law enforcement normally searches without warrants. Proportional

authorization adds internal oversight on top of existing legal requirements, and where a warrant is already legally required, it still applies.

4. Set a 30-day default retention period, with longer retention only for documented cases and lawful preservation.
5. Make the most protective applicable rule follow the data across jurisdictions.
6. Require dual authorization on both sides of interagency transfers.
7. Treat privately owned camera networks as private by default; sharing with government must be specific and affirmative.
8. Create an optional, vendor-neutral citizen portal for delayed access notices, error correction, preservation requests, and complaints.
9. Establish independent, mixed oversight boards in which the public is not outnumbered by the institutions being overseen.
10. Require vendors to build compliance into the product, meet strong cybersecurity standards, carry meaningful privacy-liability coverage, and face civil consequences for intentional or grossly negligent misuse.
11. Publish annual performance, failure, sharing, complaint, breach, and audit statistics.
12. Review the system regularly and measure whether it is solving crimes without normalizing unchecked surveillance.

Success does not mean everybody agrees. That is unrealistic. Success means law enforcement keeps a tool it can actually use, the public understands and trusts the rules, misuse is rare and quickly detected, breaches have consequences, and people stop treating camera destruction as the only form of accountability available to them.

Put bluntly: **government should mind its own business until it has a lawful, documented reason not to.** When it does have that reason, the system should help investigators move quickly. When it does not, the system should make abuse difficult, visible, and punishable.

1. Why I Am Writing This

I am writing from the middle of this argument, not from one of its extremes.

I have seen firsthand what can happen when government abuses its power. I have also seen what happens when government lacks the evidence or tools needed to hold a dangerous person accountable. I understand the technological side from my work in information technology. I understand enough of the legal and law-enforcement side to know that a good slogan does not solve an operational problem.

That is why I reject the easy answers.

I do not want a parent whose child has been abducted to hear that police refused to use a tool that could have brought that child home. I also do not want an officer, analyst, vendor employee, or outside agency to be able to reconstruct an innocent person's movements because of a grudge, a romantic relationship, curiosity, politics, or institutional convenience.

Those concerns are not mutually exclusive. In fact, a system that cannot answer both of them will eventually lose legitimacy.

My philosophy is simple: when the government has the power to seriously disrupt or destroy a person's life, it should have to prove its case and follow rules that can be verified. I would rather accept that some guilty people may escape punishment than build a system that routinely treats innocent people as searchable raw material.

That does not mean refusing modern tools. It means refusing to let technological capability become its own justification.

I do not want my children or grandchildren to inherit a society where every improvement in safety requires a matching surrender of freedom. I want them to inherit a society confident enough to use powerful tools and disciplined enough to restrain them.

That is what this paper is about.

2. What This Paper Is - and Is Not

This paper is:

- a framework for government accountability;
- a case for preserving legitimate investigative use;
- a proposal for public rules that scale with technological power;
- a technology-neutral approach that can survive changes in vendors and hardware; and
- an invitation to lawmakers, law-enforcement leaders, vendors, civil-liberties advocates, and ordinary citizens to build a workable middle ground.

This paper is not:

- a demand to abolish ALPR technology;
- an attack on law enforcement;
- a defense of any particular vendor;
- a claim that privacy always defeats public safety;
- a model bill with line-by-line statutory language; or
- a claim that courts have already resolved every constitutional question.

Flock Safety is often the company people have in mind when discussing networked license plate readers, but this paper is deliberately not about one company. Any durable policy must apply to Flock, its competitors, government-built systems, and whatever platform comes next.

3. The Tool Is Useful - and the Risk Is Real

3.1 What ALPR systems can legitimately do

An ALPR camera captures a license plate image and related information such as time, location, and vehicle characteristics. A system can compare a plate against a hot list or allow an authorized user to search historical records. The U.S. Department of Justice has identified uses that include locating stolen or suspect vehicles and assisting with Amber, Ashanti, Silver, and similar alerts. The same federal report stresses the need for clear placement and search rules, accuracy controls, encryption, access restrictions, audits, sharing protocols, and training.¹

The strongest case for ALPR use is targeted and time-sensitive:

- a child has been abducted and investigators have a vehicle description;
- a stolen car or plate triggers an alert;
- a violent crime is linked to a known plate or narrowly described vehicle;
- a missing or endangered person may be traveling in a specific vehicle;
- investigators need to corroborate a route already supported by evidence; or
- a defendant or innocent person needs location records that may support an alibi.

A trustworthy system should make these uses easier, not harder.

3.2 What changes when observation becomes infrastructure

The common defense of ALPR technology is that license plates are visible on public roads. That is true, but incomplete.

A patrol officer seeing a car at one intersection is not the same as a network of cameras recording thousands or millions of vehicles, retaining those observations, connecting them across jurisdictions, and making them searchable later. The difference is not simply what can be seen. It is **scale, persistence, aggregation, and retrospective power**.

A useful analogy is the difference between being noticed in a grocery store and being followed for a month by someone who records every stop, every companion, and every repeated pattern - then makes the notebook instantly searchable. Both begin in public. They are not the same experience, and they do not create the same power.

The U.S. Supreme Court's location-privacy cases increasingly recognize that technological scale can change the constitutional analysis. In *Carpenter v. United States*, the Court treated prolonged historical cell-site records differently from ordinary visual observation because they could reveal the "whole" of a person's movements.² In June 2026, *Chatrie v. United States* held that government acquisition of even two hours of Google Location History was a Fourth Amendment search, while leaving for further review whether each stage of the warrant was supported by probable cause and described with particularity.³

ALPR systems are not identical to cell-phone location databases. In March 2026, the U.S. Court of Appeals for the Fifth Circuit held in *United States v. Porter* that a limited local system - no more than ten cameras providing periodic public-road observations - did not amount to a Fourth Amendment search.⁴ That distinction matters. A small network producing occasional snapshots may be legally and practically different from a dense, multi-state system capable of route reconstruction and association analysis.

The legal lesson is not that every ALPR search requires a warrant today. It is that deployment density, retention, network access, query design, and analytic capability matter. Waiting for courts to draw every line after harm occurs is not a serious governance strategy.

3.3 The risks are not theoretical

Recent incidents illustrate why technical and institutional safeguards cannot be optional. In November 2025, a Georgia police chief was charged with allegedly using ALPR systems to stalk and harass people.⁵ A Pasadena, Texas, officer resigned during an investigation into alleged use of the technology to monitor another officer.⁶ Mountain View, California, reported that outside agencies accessed its camera data under sharing settings the city said it had not authorized.⁷ Separate reporting described publicly accessible live feeds and administrative controls on a limited number of misconfigured Flock camera devices; the company said the problem was limited and corrected.⁸

These examples do not prove that every agency or vendor is reckless. They prove something more basic: **misuse, misconfiguration, and security failure are foreseeable**. A sound system must be designed on that assumption.

Public frustration has also produced vandalism. Cameras were damaged in Connecticut and California in July 2026.⁹ Destroying public or private equipment is illegal, counterproductive, and often forces taxpayers or property owners to pay for replacement. But vandalism is also a warning sign. When people believe there is no legitimate path to challenge surveillance, some will choose an illegitimate path.

The answer is not to excuse destruction. The answer is to build a system whose accountability is more credible than a pair of bolt cutters.

4. The Law Is a Patchwork

There is no single nationwide ALPR rule that answers who may search, for what purpose, how long data may be held, when it may be shared, or what remedy exists after misuse. Federal agencies, states, cities, counties, and vendors operate under a mixture of constitutional doctrine, statutes, contracts, agency policies, and platform settings.

The U.S. Government Accountability Office has reported that selected Department of Homeland Security agencies had third-party access to a nationwide source of plate data, while their technology policies did not always include key privacy protections.¹⁰ GAO has also noted

both the public-safety benefits and the difficulty of measuring the effectiveness of smart-city technologies, along with concerns about transparency, data sales, privacy, and civil liberties.¹¹

State approaches vary sharply:

- Washington's 2026 law generally limits retention to 21 days, restricts private-data acquisition to a probable-cause warrant, requires vendor technical controls and sharing defaults, mandates public policies and annual reporting, and requires detailed audit trails.¹²
- Oregon's 2026 law generally uses a 30-day retention period for data not tied to an ongoing investigation or court proceeding, requires search-entry logs, limits sharing, requires recurring vendor-provided audits, and creates civil remedies for certain intentional or grossly negligent vendor misuse.¹³
- New Mexico's 2026 Driver Privacy and Safety Act restricts sharing and private-data transfer and allows a civil penalty of \$10,000 or actual damages per violation, whichever is greater.¹⁴
- Utah law allows government retention for up to nine months unless a preservation request, disclosure order, or warrant applies, while also requiring destruction as soon as reasonably possible when data is not specifically necessary for an authorized purpose. Utah also requires agency policies to be publicly available.¹⁵

These laws demonstrate that meaningful safeguards are administratively possible. They also show why a national floor is needed. A person's basic privacy should not depend entirely on which side of a county or state line a camera happens to be located.

At the same time, a federal framework must respect constitutional federalism. Congress generally cannot simply order state legislatures to enact a federal regulatory program. It can, however, regulate vendors and interstate data flows, set rules for federal agencies, create federal rights and remedies, attach appropriate conditions to federal grants, and preserve state and local authority to adopt stronger protections.¹⁶

The right architecture is therefore a **federal floor, not a federal ceiling**.

5. The SAFE Framework

SAFE is not a promise that surveillance will make every person safe. No technology can honestly make that promise. SAFE is a standard for deciding whether government surveillance is sufficiently accountable to deserve public trust. One rule runs through all four parts: whenever the system allows an exception - emergency access, an exploratory search, sharing, or extended retention - that exception must leave behind an audit trail, independent review, and identifiable responsibility.

S - Specificity

A search should begin with a lawful purpose, a documented factual basis, and the narrowest useful set of inputs. The more investigators already know - a full plate, a named suspect, a narrow time window, a particular camera, a specific crime - the less collateral exposure a request

creates.

Specificity should include:

- a case, incident, warrant, or call-for-service number;
- the authorized investigative purpose;
- the plate, partial plate, vehicle description, person, place, time, or pattern being searched;
- the time range and geographic range;
- the expected number of records or people affected, when reasonably estimable;
- the reason less intrusive methods are insufficient for a broad search; and
- a stated expiration date for alerts, hot-list entries, exports, and preserved records.

A system should not accept "because I am curious," "just checking," or a vague free-text justification. Purpose codes and required fields should be built into the workflow.

A - Authorization

Authorization should scale with the **request**, not merely with the seriousness of the case.

A child-abduction case is extremely serious, but a search for one known plate may be narrow. A lower-level investigation may involve a broad request that exposes the movements of thousands of innocent people. The second request can be more intrusive even if the underlying offense is less serious.

The governing question should be:

How much data is being requested, how many people may be affected, how specific is the request, and what inferences will the system permit?

That leads to proportional authorization. Narrow, well-supported requests require less internal approval. Broad, uncertain, historical, associative, or multi-jurisdictional requests require more.

F - Freedom

Freedom means privacy by default, due process, freedom of association, equal access to exculpatory evidence, and the right to challenge misuse.

It also means restraint. In plain language: government should mind its own business unless it has a lawful reason not to.

That principle does not prevent investigations. It prevents mission creep. Data collected for a stolen-car alert should not quietly become a general-purpose movement file. A system used to locate a missing child should not automatically become a way to map visits to homes, churches, clinics, political meetings, schools, lawyers' offices, or personal relationships.

E - Enforcement

A policy that exists only on paper is not a safeguard. The platform should enforce retention, sharing, authorization, logging, notification, and access rules automatically wherever possible.

Enforcement also requires:

- independent audits;
- public reporting;
- complaint rights;
- meaningful discipline;
- civil remedies;
- breach response;
- vendor responsibility; and
- regular public review.

The entity best positioned to prevent a violation should share responsibility for preventing it. That includes the agency, the individual user, the receiving jurisdiction, and the vendor.

6. Proportional Authorization: Trust but Verify

The most important operational reform in this paper is a simple one: **outside a sufficiently particular warrant or an exact, real-time alert governed by written policy, an ALPR search should not depend on one person's unchecked decision.**

Two-person authorization is the surveillance equivalent of two-factor authentication. We do not use two-factor authentication because every account holder is dishonest. We use it because a second independent factor makes unauthorized access harder and creates a clearer record of responsibility.

The same logic should apply to investigative searches.

6.1 Verification versus exploration

A useful distinction is the difference between **verification** and **exploration**.

Verification asks a focused question based on evidence already in hand:

- Did this known plate pass this camera during this narrow period?
- Is this exact stolen vehicle currently in the jurisdiction?
- Does this plate match the vehicle named in the warrant?

Exploration widens the net:

- Which vehicles repeatedly traveled with the suspect?
- Where does this person appear to go regularly?
- Show every black SUV in the city during a multi-hour window.
- Identify all vehicles near several sensitive locations.
- Reconstruct routes for a class of vehicles and let an algorithm rank possible suspects.

Exploration can be legitimate. It can also expose thousands of innocent people. It therefore deserves more review.

Because exploration exposes far more uninvolved people, it should require higher levels of authorization than a narrow, evidence-based query: supervisory approval, command-level approval when the request is broad or sensitive, and judicial authorization or a warrant wherever one is legally required or otherwise appropriate.

6.2 An illustrative authorization matrix

The following matrix is a policy model, not proposed statutory language. Jurisdictions should set precise thresholds publicly, within federal and state minimums.

Level	Typical request	Minimum verification
1. Exact and particularized	Exact plate, named vehicle, narrow time and place, documented case; or a sufficiently particular warrant	One authorized user when a warrant or approved exact-match workflow already supplies independent verification; complete logging required
2. Limited uncertainty	Partial plate, named person plus vehicle description, small expected result set, short historical window	Two authorized personnel must approve; one may be a peer investigator
3. Pattern or association	Route reconstruction, convoy or co-travel analysis, repeated-location analysis, cross-jurisdiction history, or a request expected to affect a substantial number of vehicles	Two-person approval plus supervisor or command-level approval; documented necessity and minimization plan
4. Broad or population-scale	Class-based search, large geographic sweep, AI analysis of thousands of vehicles, sensitive-location analysis, or any request likely to place large numbers of uninvolved people into an investigative pool	Particularized judicial authorization whenever constitutionally or statutorily available; senior command approval; automatic notice to the oversight body; strict time, use, and deletion limits

A more specific request should generally require fewer internal approvals because it exposes fewer uninvolved people. A broader request should require more approvals because it creates more risk.

6.3 The warrant relationship

A valid, sufficiently particular warrant provides an independent judicial check and can satisfy the verification baseline for the search it actually authorizes. But a warrant should not become a blank check for unlimited downstream expansion.

The Supreme Court's 2026 *Chatrrie* decision is instructive even though it concerns Google Location History rather than ALPR data. The Court emphasized that each stage of a multi-step location search must be evaluated for particularity and probable cause.¹⁷ The policy lesson is

clear: when a search begins broad and investigators later select which people receive deeper scrutiny, the later stages need their own limits and accountability.

6.4 Emergencies should not swallow the rule

"Emergency" and "for your safety" are among the easiest phrases to abuse in government. A framework that suspends all safeguards whenever someone checks an emergency box does not have safeguards.

In most genuine emergencies, multiple officers, dispatchers, supervisors, neighboring agencies, or command staff are already involved. A rapid second approval can be completed electronically or by phone. A rural deputy working alone should be able to obtain remote approval from a supervisor, dispatch commander, state fusion center, or neighboring jurisdiction.

The rule should therefore be:

- urgent searches receive an expedited workflow, not unilateral immunity;
- a second approver remains required whenever technically possible;
- the system records who invoked urgency and why;
- any temporary exception expires quickly;
- the oversight body receives automatic notice; and
- mandatory after-the-fact review of every emergency search determines whether the emergency designation was justified.

This after-the-fact review should be mandatory for every emergency search, and it should be a federal minimum requirement rather than a local option. An emergency exception that no one is required to review afterward is exactly how "emergency" becomes a permanent loophole.

Law enforcement solved emergencies before ALPR networks existed. A short verification step is a reasonable price for giving government vastly greater reach afterward.

6.5 Hot lists and alerts

Hot-list entries can turn a narrow investigation into continuous automated monitoring. They should therefore include:

- a specific lawful purpose;
- the entering user's identity;
- the approving user's identity when dual authorization applies;
- a case or warrant number;
- a start date and automatic expiration;
- a requirement to confirm that the underlying warrant, stolen status, or safety alert remains active; and
- periodic review of long-running entries.

An automated alert should be treated as an investigative lead, not as conclusive proof. Washington and Oregon now require visual or independent confirmation before a stop based on an ALPR alert, reflecting a sound accuracy principle.¹⁸

7. Data Governance: Collection, Access, Use, Retention, and Deletion

Surveillance policies often use the word "data" as though every event in the data lifecycle were the same. They are not.

A serious policy should separately define:

- **capture:** the camera creates a plate record;
- **access:** a user opens or retrieves a record;
- **search:** a user submits inputs to locate records;
- **view:** a user sees returned information;
- **collection into a case:** a record is affirmatively associated with an investigation;
- **export or download:** a copy leaves the ordinary platform view;
- **sharing:** another person, agency, or vendor receives access or a copy;
- **analysis:** software or a person infers routes, associations, or patterns;
- **preservation:** normal deletion is paused for a defined legal reason;
- **retention:** the data continues to exist after its ordinary period; and
- **deletion:** the record and accessible copies are rendered unrecoverable, subject to narrowly defined backup rules.

Each event should have its own rule and audit entry.

7.1 A 30-day default

Thirty days is a reasonable national maximum for ordinary plate records that have not been incorporated into a documented investigation. Oregon adopted a 30-day limit in 2026 for data not connected to an ongoing investigation or court proceeding. Washington chose an even shorter general period of 21 days. Flock states that many customers use a 30-day default, subject to local law and contract.¹⁹

A federal floor should require:

- automatic deletion no later than 30 days after capture for ordinary records;
- authority for states and localities to require a shorter period;
- no extension merely because data was transferred to another agency;
- no manual "just in case" archive; and
- auditable proof that deletion occurred.

Data specifically connected to a documented investigation, litigation hold, preservation request, or court order may be retained longer, but only for the period reasonably necessary. Once the case or legal basis ends, the data should return to an applicable records schedule and be deleted rather than drifting into permanent storage.

Deletion must never become a tool for concealment. No user, agency, or vendor should be able to intentionally delete records, or accelerate their destruction, in order to hide misconduct. Once data becomes relevant to an open investigation, complaint, audit, disciplinary review, litigation, or criminal matter, automatic deletion must immediately stop for that data, which must then be preserved until the matter is fully resolved.

7.2 Preservation must be narrow and symmetric

Preservation should identify the plate, camera, place, date, time range, or other specific data to be held. It should not freeze an entire database.

The right to seek preservation should not belong only to prosecutors. A defendant, defense attorney, victim, or person with a credible need to preserve possible exculpatory or alibi evidence should have access to a neutral process. Utah law already recognizes preservation and disclosure mechanisms that can be invoked by a governmental entity or a defendant in a criminal case.²⁰

A fair system helps prove guilt when evidence supports guilt and helps prove innocence when evidence supports innocence.

7.3 The most protective rule follows the data

Data should carry its protections with it.

If a plate record is captured in a jurisdiction with a 15-day retention limit, another jurisdiction should not be able to request the record and restart the clock at 30, 90, or 270 days. If the originating jurisdiction bars a particular use or requires a warrant for private data, transfer should not erase that rule.

The governing principle should be:

No transfer may dilute the protections attached to the data at the place and time of collection.

Where several rules apply, the most protective rule should control unless a court specifically authorizes a lawful extension. This creates both a chain of custody and a **chain of privacy continuity**.

7.4 Sensitive locations and protected activity

Systems should not be used to identify, catalog, or infer lawful participation in constitutionally protected activity. Searches centered on houses of worship, schools, medical facilities, legal offices, political meetings, protests, shelters, or other sensitive locations should require heightened approval and a clearly documented nexus to a specific investigation.

A broad request should not become lawful simply because a crime occurred somewhere inside the search area. Location, time, and data categories must still be narrowed. Washington's 2026 law offers one current example of restrictions around several sensitive locations and protected activity.²¹

7.5 Data quality and correction

An ALPR match can be wrong because of glare, plate damage, temporary tags, character confusion, stale hot-list data, stolen plates, vehicle transfers, or human entry error. Policies should require:

- updated source databases;
- visual verification before enforcement action;
- a way to flag and correct erroneous records;
- notice to agencies that received corrected data;
- quality testing across conditions and plate types; and
- documented review when a bad alert contributes to a stop, search, arrest, or other harm.

Errors are not merely technical defects. In this context, they can become police encounters.

8. Interagency Sharing: A Chain of Authorization

Data sharing is where local promises can quietly become national surveillance.

A city may adopt a strict policy, only to discover that a platform setting, regional agreement, vendor update, or broad credential allows dozens or hundreds of outside agencies to search its records. That defeats local control.

8.1 Dual authorization at every trust boundary

When one agency requests another agency's data, there should be verification on both sides:

- two authorized people at the requesting agency approve the request;
- two authorized people at the receiving agency approve release or access;
- both sides record the case number, purpose, scope, time range, and legal authority;
- both sides retain an immutable audit record; and
- both sides remain responsible for compliance.

This is not bureaucratic theater. It makes collusion harder, creates shared accountability, and reduces the chance that one person can use a national network to check on a spouse, former partner, colleague, neighbor, political critic, or private citizen.

8.2 No automatic nationwide access

Sharing should be specific, not ambient.

An agency should not receive nationwide search access merely because it purchases the same product as another agency. A reciprocal network can be useful, but participation should require an affirmative public decision, a written agreement, defined purposes, named participating agencies or categories, expiration and renewal, and technical settings that default to no sharing.

Washington's 2026 law now requires vendor controls against unauthorized sharing and directs vendors to default sharing settings against access by unauthorized entities.²² That is the right design principle: local policy should be reflected in the software, not contradicted by it.

8.3 Interstate requests

An out-of-state request should include:

- the requesting agency and user identities;
- the investigation and offense category;
- a case number;
- the data sought;
- the legal authority;
- an agreement to follow the originating jurisdiction's restrictions; and
- an audit and notification commitment.

If the requesting jurisdiction would use the data for a purpose prohibited where it was collected, the request should be denied unless a controlling court order requires otherwise.

9. Private Camera Networks: Private by Default

A grocery store, church, hardware store, homeowners association, apartment complex, or other private entity may choose to install a camera system. That does not mean its data should automatically become part of a government network.

The default should be private.

A private organization may affirmatively opt in to share with a specific jurisdiction for defined purposes and a defined period. That decision should not silently authorize every local, state, and federal agency using the same vendor.

Throughout this framework, the "owner" of a camera system means the entity that exercises operational control over the data, not merely whoever holds legal title to the hardware. If a vendor such as Flock owns the physical equipment but a city leases and operates it, the city - not the vendor - controls sharing decisions and carries the corresponding responsibility. Control follows operational authority, not the invoice.

The 30-day default retention limit applies to government-held or government-accessible data. It does not require a private owner to delete their own footage. A store, church, or homeowners association remains free to keep its own recordings longer - at its own expense and for its own purposes - provided the data stays private and is not shared with, or made accessible to, government except through the affirmative consent or lawful process described here.

A sound policy should require:

- written, informed, revocable consent by the private owner;
- identification of the specific agency or agencies receiving access;
- a public description of the sharing program, while protecting genuinely sensitive security details;
- the same retention, audit, use, and breach rules that apply to government-collected data once government accesses it;
- no resale or secondary sharing; and
- a warrant or other valid court process when the private owner has not opted in.

New Mexico's 2026 law provides one example by requiring the private owner's express consent or a valid court order before privately captured ALPR information is released. Washington requires a probable-cause warrant for privately held ALPR data.²³

Private consent should also be revocable. Ending participation should disable future access and trigger deletion of records not lawfully preserved.

10. Citizen Rights: Personal Transparency Without Compromising Cases

Most surveillance transparency is institutional: agencies publish a policy or an annual report. That is necessary, but it does not answer the question an individual naturally asks: **Was my information used?**

A modern accountability system should offer an optional, vendor-neutral privacy portal administered by an independent public office or trusted service.

10.1 The opt-in privacy portal

A citizen who chooses to participate should be able to verify identity, establish a lawful connection to a vehicle or plate, and enroll for delayed notices. Enrollment should be voluntary. The person should be able to leave the program at any time.

The portal should provide notice when the enrolled plate is:

- queried in a historical search;
- returned in a pattern or association analysis;
- exported or downloaded;
- shared with another jurisdiction;
- placed on a hot list;
- preserved beyond the default retention period; or
- used as evidence in a case, subject to lawful delay and redaction.

The portal should not become a live "who is investigating me" service. Notices should ordinarily be delayed for at least 60 days, as a policy starting point. An investigator may seek a court-approved extension when notice would materially risk a specific investigation, witness, victim, or safety operation. Every extension should be documented, time-limited, and eventually reviewable.

10.2 Law enforcement should not see who opted in

Opt-in status should be hidden from ordinary investigators. Otherwise, enrollment itself could become a signal or alter investigative behavior.

The platform should send audit events to the independent notification service. The service, not the officer, determines whether and when a notice is delivered. Disclosure of enrollment status should require specific legal authority.

This arrangement is technically realistic. Modern systems already separate roles, permissions, logs, and automated workflows. The challenge is governance, not basic computing.

10.3 Security for the portal

A portal containing personal access notices could itself become a surveillance target. It should therefore require:

- strong identity proofing;
- hardware-backed or equivalent multi-factor authentication;
- alerts for account changes;
- strict limits on delegated access;
- separate storage of enrollment identity and law-enforcement search records;
- encryption and tamper-evident logs;
- rapid revocation after vehicle sale, plate change, death, or fraud; and
- independent penetration testing.

The portal should reveal only what the law permits. It should not expose protected witness information, undercover operations, or another person's private data.

10.4 Additional individual rights

Every person should have a clear right to:

- learn the governing policy and retention period;
- request correction of a demonstrably inaccurate record;
- receive delayed notice when enrolled;
- file a complaint directly with the independent oversight body;
- request review of an apparent unauthorized search;
- seek preservation of potentially exculpatory records through a neutral process;
- obtain records through discovery or lawful process when relevant to a defense or claim;

- be informed after a material breach involving their data when identification is reasonably possible; and
- seek a meaningful remedy when intentional or grossly negligent misuse causes harm.

Transparency should not be limited to people with the time and money to hire a lawyer and file repeated public-records requests.

11. Independent Oversight: Every Affected Voice at the Table

Oversight cannot be credible if the same institution that approved a search is the only institution allowed to investigate it.

Complaints should go directly to an independent oversight body. A complainant should not be required to first ask the agency they distrust to investigate itself.

11.1 Required representation

Balanced representation is a design requirement, not a preference.

The board should include experience from:

- the general public, including members unaffiliated with law enforcement or vendors;
- law-enforcement operations;
- internal affairs, professional standards, or comparable compliance work;
- prosecution, defense, civil law, or judicial administration;
- privacy, cybersecurity, data governance, or information technology;
- local or state government administration; and
- communities directly affected by deployment.

No institutional bloc should control the board. Unaffiliated civilian members should hold at least a plurality, and preferably a majority, because the public is the party whose movements are being recorded. One civilian seat should be reserved for a person with a demonstrated history of raising public concerns about surveillance or government accountability, not merely a person selected because they are unlikely to challenge the system.

11.2 Scale and structure

Board size can scale with jurisdiction. An illustrative model is:

- local or small-city body: at least 3 members;
- county or regional body: at least 5 members;
- state body: at least 7 members; and
- federal body: 9 members.

Larger boards may be appropriate. The essential requirements are an odd number, mixed representation, public appointment rules, and no law-enforcement or vendor majority.

Terms should be staggered and limited, with two-year terms as a reasonable starting point. Members should disclose conflicts, gifts, vendor relationships, campaign interests, employment ties, and close personal connections to agencies under review.

11.3 Authority

An oversight body should be able to:

- receive and investigate complaints;
- compel production of audit logs and policies, subject to lawful confidentiality;
- refer suspected crimes to an independent prosecutor or inspector general;
- order or recommend corrective action;
- publish findings and aggregate statistics;
- review broad-search notices and emergency exceptions;
- conduct random and risk-based audits;
- review contracts and material vendor changes;
- recommend policy updates as technology evolves; and
- hear appeals or transmit them to the next level of review.

The appeal structure should be understandable. A local decision may be appealed to a state body, and a state decision involving federal rights may be reviewed through an appropriate federal administrative or judicial process. The exact route will vary, but no agency should have the last word on its own alleged misuse.

11.4 Open governance

Board charters, membership, meeting schedules, policies, non-sensitive minutes, audit summaries, and final decisions should be public. Closed sessions should be narrow and justified by a specific need, such as an active investigation, protected personnel matter, victim privacy, or classified information.

Public input should occur before first deployment, before major expansion, before new analytic capabilities are activated, and during periodic review.

12. Vendor Responsibility: Compliance by Design

Government agencies operate the system, but vendors often control the architecture. A vendor may determine how retention is configured, what sharing defaults exist, what logs are available, how permissions work, whether a user can export data, and whether a software update changes the risk.

It is therefore not enough to regulate only the officer at the keyboard.

12.1 Required technical controls

Contracts and law should require the vendor to implement:

- role-based access;
- purpose and case-number fields before a search runs;
- proportional approval workflows;
- time-limited hot lists;
- sharing defaults set to off;
- jurisdiction-specific retention;
- automatic deletion;
- immutable or tamper-evident audit logs;
- export and download logging;
- configurable sensitive-location restrictions;
- cross-jurisdiction policy enforcement;
- delayed notification interfaces;
- strong encryption in transit, at rest, and where feasible on-device;
- rapid credential revocation;
- secure backup and deletion rules;
- independent security testing; and
- documented incident response.

An agency should not be able to waive a statutory safeguard with a checkbox. A vendor should not be able to change a sharing setting or expand a feature without explicit customer authorization, advance notice, and a new privacy review when the change is material.

12.2 Data ownership and secondary use

The vendor should have no independent right to sell, license, advertise with, train unrelated models on, or otherwise monetize government ALPR data. Technical support access should be limited to the time and purpose authorized and fully logged.

The vendor's public statements about privacy should be enforceable through contract. Marketing promises should not disappear in fine print.

12.3 Cybersecurity and breach duties

Minimum duties should include:

- recognized security and privacy management standards;
- recurring independent audits;
- coordinated vulnerability disclosure;
- prompt remediation timelines based on severity;
- notice to affected customers and oversight bodies;
- preservation of forensic evidence;
- after-action reports for material incidents;

- customer access to relevant audit findings; and
- clear rules for subcontractors and cloud providers.

A vendor certification is evidence, not immunity. The December 2025 reporting about exposed camera feeds illustrates why configuration, deployment, and ongoing monitoring matter in addition to central-platform controls.²⁴

12.4 Financial responsibility

An entity that profits from collecting and managing sensitive location data should be financially capable of responding when negligent security or improper disclosure harms people.

Vendors should carry cyber and privacy liability insurance, a bond, or another approved financial-responsibility mechanism. The required amount should scale with factors such as:

- number of deployed devices;
- volume of records;
- number of connected jurisdictions;
- breadth of sharing;
- types of analytics offered;
- history of incidents; and
- likely cost of notice, remediation, identity protection, legal claims, and reputational harm.

Insurance should not replace liability or become a license to be careless. It should ensure that a valid claim does not become worthless because the responsible company lacks accessible funds.

Oregon's 2026 law creates a civil action for certain intentional or grossly negligent vendor access, disclosure, sale, sharing, or use. New Mexico's 2026 law authorizes enforcement authorities to seek injunctive relief and a civil penalty for intentional sharing violations, and it permits corrective action or termination of vendor access for noncompliance. Those approaches show that vendor accountability is not merely theoretical.²⁵

12.5 Allocation of responsibility

Liability should follow control and culpability:

- the user is responsible for an intentional personal search;
- the agency is responsible for weak supervision, unlawful policy, or failure to respond to warnings;
- the receiving agency is responsible for unauthorized secondary use;
- the vendor is responsible for insecure design, unauthorized access, undisclosed changes, or misuse within its control; and
- multiple parties may share responsibility when their failures combine.

A contract should not allow one party to shift all public harm to another through indemnity language that citizens never see.

12.6 Physical deployment and roadway safety

Vendor responsibility should extend beyond cybersecurity to the physical safety of the hardware itself. ALPR cameras and their poles are frequently installed in and beside public roadways, where a poorly engineered installation can endanger drivers. Vendors and installers should be required to comply with applicable Department of Transportation requirements, breakaway-pole standards, roadway clear-zone and safety regulations, and other relevant engineering standards for roadside equipment. A vendor's obligations do not end at the data layer; safe physical deployment is part of doing this work responsibly.

13. Transparency: Publish the Whole Picture

A jurisdiction should not ask the public to trust a system while refusing to explain how it is used.

Every agency's ALPR or automated-surveillance policy should be a public document, posted in a predictable place and written clearly enough for a non-lawyer to understand. Utah and Washington already require public availability of agency policies in different forms.²⁶

13.1 Annual public report

At minimum, each jurisdiction should publish:

- number and general locations of cameras, with narrowly justified exceptions;
- number owned, leased, or controlled by government;
- number owned by private entities and shared with government;
- total plate reads;
- total searches;
- alerts generated;
- searches that yielded results;
- searches that produced no useful lead;
- exact-match versus partial, pattern, association, or broad searches;
- warrants, court orders, and preservation requests;
- interagency requests received, approved, modified, and denied;
- identities or categories of outside agencies receiving access;
- records exported, downloaded, or shared;
- stolen vehicles and plates recovered with assistance from the system;
- missing or endangered persons located with assistance from the system;
- cases in which the system materially assisted an arrest, prosecution, dismissal, defense, or exoneration;
- confirmed false alerts or material data errors;
- complaints, audit findings, policy violations, discipline, and criminal referrals;

- breaches, exposures, and material security incidents;
- average and maximum retention periods actually used;
- number and reason for retention extensions;
- emergency designations and the result of after-action review;
- vendor changes affecting collection, sharing, analytics, or retention; and
- cost of the system, including replacement, litigation, audit, and incident-response costs.

Washington's 2026 law requires annual reporting that includes reads, searches that yielded results, alerts, stolen-vehicle recoveries, prosecutions, sharing, warrants, policy changes, audits, and camera locations. That is a strong starting point.²⁷

13.2 Report failure as well as success

Agencies naturally publicize cases where technology helped. They should also disclose how often it did not help.

A search that produces no useful lead is not automatically a failure; ruling out possibilities has investigative value. But the public cannot assess effectiveness if it sees only success stories. GAO has noted that the costs and benefits of smart technologies can be difficult to measure and isolate.²⁸

Honest reporting should distinguish:

- direct causal assistance;
- corroborating assistance;
- no material contribution;
- false or stale alerts;
- investigative dead ends; and
- cases in which the data supported an alibi or corrected an initial suspicion.

13.3 Public camera notice

Visible signage may be appropriate where cameras monitor entrances, parking areas, parks, or other defined property. A sign should identify the type of system, the owner, the public policy, and where to learn more. Roadway deployments may require different notice methods, such as a public map and council-approved deployment plan.

Notice does not cure an unlawful search. It does improve honesty and public awareness.

14. Misuse, Discipline, and Remedies

Rules without consequences invite contempt. Consequences without due process invite injustice. A credible system needs both.

14.1 Distinguish types of failure

Policy should distinguish:

1. **Intentional misuse:** searching for a romantic partner, former partner, colleague, critic, neighbor, family member, or other person for a non-law-enforcement purpose; falsifying a justification; sharing data for retaliation, profit, embarrassment, politics, or harassment.
2. **Gross negligence:** ignoring clear rules or warnings in a manner that creates a serious and obvious risk.
3. **Ordinary negligence or policy error:** failing to follow a procedure without malicious intent.
4. **Good-faith technical or factual error:** acting reasonably on incorrect system information or a genuine misunderstanding.
5. **Exceptional operational circumstance:** a rare event in which an officer deviated from procedure to address an immediate threat and the deviation is promptly disclosed and independently reviewed.

These categories should not be defined by whether the search happened to find a guilty person. A search is not made proper by what it turns up. Allowing the result to excuse the method creates the exact incentive that safeguards are meant to prevent.

14.2 Proportionate consequences

Potential consequences should include:

- retraining and corrective action for minor, good-faith mistakes;
- temporary access suspension;
- formal discipline;
- loss of system privileges;
- employment consequences for serious or repeated violations;
- license or certification review where applicable;
- evidence consequences under existing law;
- civil liability and damages;
- attorney fees and injunctive relief;
- criminal referral for stalking, harassment, official misconduct, unauthorized computer access, obstruction, falsification, or related conduct; and
- vendor penalties, contract termination, or debarment.

Intentional personal misuse should be treated as a serious abuse of office, not a minor policy infraction.

14.3 No retaliation

Whistleblowers, auditors, complainants, defense attorneys, journalists, and public employees who report suspected misuse in good faith should be protected against retaliation. Anonymous or confidential reporting channels should be available, with penalties for knowingly false

complaints but not for good-faith reports that cannot ultimately be proven.

14.4 Breach compensation

When a breach or unauthorized disclosure exposes a person's movements or private associations, the harm may be difficult to price. A victim should not have to prove identity theft before the law recognizes an injury.

Remedies may include:

- actual economic and noneconomic damages;
- a reasonable statutory minimum for proven violations;
- injunctive relief;
- correction and deletion;
- notice and protective services;
- reasonable attorney fees; and
- access to a vendor or agency insurance claim process.

The exact amounts belong in legislation. The principle belongs here: **the people exposed should not carry the entire cost of someone else's failure - whether that failure lies in jurisdiction negligence, agency negligence, or vendor negligence.**

15. A Federal Floor With State and Local Control

The framework should be layered.

15.1 Federal responsibilities

Federal law should establish minimum rights and obligations for:

- federal-agency use of ALPR and comparable automated surveillance;
- vendors engaged in interstate commerce;
- interstate data transfers;
- baseline retention, security, audit, notice, and remedy requirements;
- federal grant conditions for agencies that purchase or operate the systems;
- national technical standards and interoperability; and
- protection of stronger state and local rules.

The federal standard should be a floor. It should not preempt a state or city that chooses shorter retention, narrower sharing, stronger notice, more approvals, or broader remedies.

Because Congress cannot simply command states to pass particular legislation, the federal framework should regulate covered conduct directly where constitutionally authorized and use appropriate funding conditions rather than pretending federalism does not exist.²⁹

15.2 State responsibilities

Each state should be required, as a condition of relevant federal funding and system participation, to publish a statewide framework addressing:

- authorized uses;
- minimum approval tiers;
- retention and preservation;
- private networks;
- interagency and interstate sharing;
- sensitive locations;
- oversight and appeals;
- public reporting;
- citizen rights;
- remedies; and
- vendor requirements.

States may go beyond the federal floor. They should also establish how purely private surveillance networks are governed even when government does not access them. That private-sector question may involve different rules, but it should not be ignored.

15.3 Local responsibilities

A city, county, sheriff's office, police department, transportation agency, or other local user should adopt a public policy before deployment. The policy must fit within federal and state protections and may be more protective.

Local policy should identify:

- deployment locations or location criteria;
- authorized users;
- approval thresholds;
- retention;
- sharing partners;
- private-camera participation;
- complaint routes;
- oversight board jurisdiction;
- annual reporting; and
- review dates.

Local debate is not a nuisance. It is part of legitimacy. People are more likely to accept a system when they can see who approved it, which rules apply, and how those rules can be changed.

15.4 Periodic review

Technology changes faster than statutes. Every policy should undergo a full public review at least every two years and sooner when there is:

- a material security incident;
- a new analytic feature;
- a major vendor or contract change;
- expansion into a new category of location or data;
- evidence of repeated misuse;
- a significant court ruling; or
- a substantial change in state or federal law.

A review should ask whether the system is still necessary, effective, proportionate, secure, and consistent with community expectations.

16. Strong Counterarguments - and Straight Answers

16.1 "You have no privacy on a public road"

A person has less privacy in a public place than in a home. That does not answer whether government may retain and aggregate observations into a searchable history without meaningful limits.

The point is not to pretend a license plate is secret. The point is that an officer's eyes and a networked historical database are not equivalent merely because both begin with something visible in public.

16.2 "Two-person approval will slow emergencies"

A rapid second approval is modest compared with the reach the technology provides. In serious emergencies, multiple personnel are usually involved. Remote approval can serve rural and overnight operations. The workflow can take seconds, not hours.

The alternative is a unilateral emergency exception that can be invoked whenever rules become inconvenient. That is not a safeguard.

16.3 "Criminals will benefit from privacy rules"

Any rule of evidence, warrant requirement, access control, or due-process protection may make some investigations harder. That is not an accidental flaw in a free society. It is the cost of requiring government to prove its case through lawful means.

The SAFE Framework preserves exact alerts, warrant-based searches, targeted investigation, urgent response, and lawful pattern analysis. It does not protect criminals from investigation. It protects everyone from unaccountable investigation.

16.4 "Existing internal affairs and logs are enough"

Logs help only if they are complete, reviewed, retained, and available to someone independent of the user and chain of command. Internal affairs can play an important role, but it should not be the only route for a complaint about the institution itself.

Recent misuse allegations and sharing disputes show why independent oversight and technical controls are needed in addition to policy.³⁰

16.5 "This creates too much bureaucracy"

Most of the proposed friction can be automated: required fields, second approval, expiration, audit alerts, delayed notice, and deletion. These controls are ordinary concepts in banking, health care, cloud security, nuclear operations, and other high-trust systems.

The relevant comparison is not zero cost. It is the cost of safeguards versus the cost of misuse, litigation, breaches, damaged careers, lost public trust, contract termination, and destroyed cameras.

16.6 "Local communities should decide everything"

Local control matters, but movement data crosses local boundaries. Vendors and networks operate across states. A community with strong rules can have its protections weakened by an outside search or transfer.

A national floor is not only a rights protection; it is also a practical benefit. Consistent minimum standards reduce friction when agencies legitimately need to share data, create predictable expectations for the public and for law enforcement nationwide, and simplify interoperability across systems and vendors. They also prevent a jurisdiction from gradually sliding into an unchecked surveillance state simply because the places around it adopted weaker safeguards. Consistency improves privacy protection and operational efficiency at the same time.

A federal floor protects basic rights. State and local governments remain free to do more.

16.7 "A good detective sometimes has to bend the rules"

Rules should be designed so a good detective rarely needs to choose between procedure and safety. There should be expedited approvals and clear exceptional-circumstance review.

But the outcome cannot be the test. If breaking the rule is forgiven whenever it produces a serious arrest, every investigator is encouraged to gamble with other people's rights. The system should distinguish good-faith error from intentional abuse without adopting "the ends justify the means" as policy.

17. What Success Looks Like

Success is not unanimous agreement. It is not a world without crime, mistakes, lawsuits, or criticism. It is a stable system that the broad middle of the public and law enforcement can live with.

Five years after adoption, success should look like this:

- **Law enforcement still wants the tool.** Investigators can use it quickly for exact alerts, documented cases, missing persons, stolen vehicles, and appropriately approved analysis.
- **The public is no longer in a permanent fight over whether the cameras should exist.** People know the rules, the policies are public, complaints have a credible route, and camera vandalism becomes rare rather than a recurring form of protest.
- **Misuse is difficult and visible.** Personal searches, false justifications, unauthorized sharing, and improper retention are detected through controls and audits.
- **Breaches are rare, contained, disclosed, and compensated.** Vendors and agencies have a strong incentive to prevent them.
- **Broad searches are exceptional.** When they occur, the record shows who approved them, how many people were affected, what the search accomplished, and when the data was deleted.
- **Good cases move faster.** The safeguards are built into the workflow instead of handled through improvised paperwork.
- **Innocent people can use the system too.** Exculpatory data can be preserved, errors can be corrected, and delayed notices make secret misuse harder.
- **The debate improves.** Public meetings focus on performance, policy, and upgrades instead of cycling endlessly between "ban everything" and "trust us."

The ultimate measure is not how many cameras are installed. It is whether public safety improves without making ordinary people feel that their government is keeping a private map of their lives.

18. SAFE Principles for Responsible Public Surveillance

These principles are meant to be remembered, repeated, and applied beyond license plate readers.

1. **Power demands accountability.** The stronger the capability, the stronger the check.
2. **Trust but verify.** Legitimate users may act, but no sensitive use should be invisible or solely self-approved.
3. **Be specific.** Search for what the evidence supports, not everything the technology can reach.
4. **Mind your own business by default.** Government should not investigate lawful life without a documented lawful reason.
5. **Protect the innocent while pursuing the guilty.** A useful tool must support exoneration and alibis as well as prosecution.
6. **Make privacy travel with the data.** Sharing may not weaken the rule or restart the clock.
7. **Keep private systems private by default.** Government access requires affirmative consent or lawful process.
8. **Put every affected voice at the table.** Public, law-enforcement, legal, technical, and civil perspectives belong in governance.

9. **Build the rule into the machine.** Retention, approval, sharing, and audit requirements should not depend on memory or goodwill.
10. **Make abuse costly.** Intentional misuse, negligent security, and unauthorized disclosure require real consequences.
11. **Publish both success and failure.** Public value cannot be measured through success stories alone.
12. **Review the system before the system becomes permanent.** Technology, law, and community expectations change.

19. Questions Every Community Should Ask

Before approving, renewing, or expanding an automated public-surveillance system, citizens and lawmakers should ask:

1. What exact problem is this system meant to solve?
2. Which uses are permitted, and which are prohibited?
3. Who can search the system?
4. What must a user enter before a search runs?
5. Which searches require a second person, a supervisor, senior command, or a judge?
6. How does approval scale with the number of people affected and the amount of data requested?
7. What is the default retention period?
8. What legal event allows longer retention, and who confirms deletion afterward?
9. Does the strictest applicable rule follow the data when it is shared?
10. Which outside agencies can access local records, and is sharing off by default?
11. Are privately owned cameras private by default?
12. Are sensitive locations and protected activities subject to heightened rules?
13. Can a citizen learn, after an appropriate delay, whether their data was searched or shared?
14. Can a defendant or innocent person preserve records that may prove an alibi?
15. Who investigates a complaint against the agency?
16. Is the oversight body independent, mixed, transparent, and appealable?
17. What happens to an officer who searches an ex-partner, colleague, critic, or neighbor?
18. What happens when a vendor's design, update, employee, subcontractor, or security failure causes harm?
19. Does the vendor carry enough insurance or financial responsibility to pay valid claims?
20. What statistics will be published every year, including unsuccessful searches and false alerts?
21. Has the jurisdiction shown that the system is worth its financial and privacy cost?
22. When will the public get to reconsider the policy?

23. As the technology grows more powerful, will our commitment to liberty and accountability grow with it?
24. What kind of society do we want our children and grandchildren to inherit?

Conclusion

The question is not whether technology will become more powerful. It will.

The question is whether public accountability will keep pace.

Automated license plate readers can help bring an abducted child home. They can help recover stolen property, identify a dangerous suspect, and support an innocent person's alibi. Those benefits deserve to be taken seriously.

So do the risks.

A government that can reconstruct movement, association, and routine has a power earlier generations could not easily exercise at scale. That power should not rest on a vendor setting, an unpublished department memo, or the personal restraint of whoever happens to have a login.

The public should not be asked to choose between blind trust and destroying cameras. Law enforcement should not be asked to choose between effective tools and public legitimacy. Vendors should not be permitted to collect public money while shifting the cost of failure onto the people whose data they hold.

We can build something better: a system where narrow, lawful investigations move quickly; broad searches require broader accountability; data expires; protections travel; private networks remain private unless deliberately shared; citizens have rights; oversight includes every affected voice; and abuse carries consequences.

That is not anti-technology. It is not anti-police. It is what responsible government looks like in a technological age.

Power demands accountability.

Glossary

Access: Opening, retrieving, or otherwise obtaining the ability to view or use a system or record.

ALPR / LPR: Automated license plate reader or license plate reader; a camera and software system that converts plate images and related vehicle observations into searchable data.

Analysis: Manual or automated processing that infers routes, associations, patterns, rankings, or other conclusions from records.

Authorization: Approval required before a search, access, transfer, export, preservation, or other action.

Broad search: A query expected to affect a large number of vehicles or people, or one that begins with limited specificity and relies on filtering or analytics to identify possible subjects.

Capture: Creation of a plate record by a camera or related system.

Chain of authorization: The documented approvals attached to a request and transfer, including both requesting and releasing parties.

Collection into a case: Associating a returned record with a particular investigation, proceeding, intelligence file, or official record.

Export / download: Creation of a copy outside the normal platform view or transfer into another system.

Hot list: A list of plates or vehicle characteristics that generates an alert when a match occurs.

Most protective rule: The shortest retention, narrowest permitted use, strongest approval, or other highest privacy protection among the rules legally attached to the data.

Oversight body: An independent, mixed public body authorized to receive complaints, conduct audits, review policy, and make or recommend findings and remedies.

Preservation: Temporary suspension of ordinary deletion for specifically identified data under documented legal authority.

Proportional authorization: A system in which approval requirements increase with the breadth, uncertainty, amount of data, sensitivity, and number of people affected by a request.

Retention: Continued storage or availability of data after capture.

Search: Submission of information or criteria to retrieve, compare, rank, filter, or analyze records.

Sensitive location: A place where surveillance may reveal highly private or constitutionally protected activity, including certain medical, religious, educational, legal, political, residential, shelter, or social-service locations.

Sharing: Allowing another user, agency, vendor, or entity to access, receive, query, or obtain data.

Use: Reliance on data for an investigative, enforcement, administrative, evidentiary, intelligence, or decision-making purpose.

Vendor: A private entity that provides cameras, software, storage, analytics, network access, support, or related surveillance services.

View: Display of a record or search result to a user, whether or not it is downloaded or placed into a case.

Footnotes

1. U.S. Department of Justice, Office of Legal Policy, *Artificial Intelligence and Criminal Justice: Final Report* (Dec. 3, 2024), pp. 26-28, <https://www.justice.gov/olp/media/1381796/dl>. ↵
2. *Carpenter v. United States*, 585 U.S. 296 (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. ↵
3. *Chatrpie v. United States*, No. 25-112, 609 U.S. ___ (June 29, 2026), https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf. ↵
4. *United States v. Porter*, No. 25-60163 (5th Cir. Mar. 17, 2026), <https://law.justia.com/cases/federal/appellate-court/s/ca5/25-60163/25-60163-2026-03-17.html>. ↵
5. Associated Press, "Georgia police chief charged with using license plate readers to stalk and harass people" (Nov. 20, 2025), <https://apnews.com/article/georgia-plate-readers-stalk-harass-chief-arrested-39adb6f89fc2074da61f2801fef3f180>. ↵
6. KPRC 2 (Click2Houston), "Pasadena police sergeant resigns while under internal investigation; council member cites alleged misuse of Flock camera" (July 10, 2026), <https://www.click2houston.com/news/local/2026/07/10/pasadena-police-sergeant-resigns-while-under-internal-investigation-council-member-cites-alleged-misuse-of-flock-camera/>. ↵
7. ABC7 San Francisco, "Mountain View officials allege federal, state agencies accessed Flock camera data without consent" (Feb. 1, 2026), <https://abc7news.com/post/city-mountain-view-alleges-federal-state-agencies-accessed-flock-safety-camera-data-consent/18518963/>. ↵
8. The Verge, "Dozens of Flock AI camera feeds were just out there" (Dec. 2025), <https://www.theverge.com/news/849624/flock-ai-camera-feeds-exposed-benn-jordan>. ↵
9. CT Insider, "Milford Flock license plate cameras damaged in apparent vandalism, police say" (July 23, 2026), <https://www.ctinsider.com/news/milford/article/milford-flock-cameras-damaged-vandalism-22357695.php>; San Francisco Chronicle, "California man accused of intentionally running over Flock cameras" (July 28, 2026), <https://www.sfchronicle.com/california/article/flock-camera-vandalism-arrest-22364531.php>. ↵
10. U.S. Government Accountability Office, *Law Enforcement: DHS Could Better Address Bias Risk and Enhance Privacy Protections for Technologies Used in Public*, GAO-25-107302, <https://www.gao.gov/products/gao-25-107302>. ↵
11. U.S. Government Accountability Office, *Smart Cities: Technologies and Policy Options to Enhance Services and Transparency*, GAO-25-107019 (Apr. 30, 2025), <https://www.gao.gov/products/gao-25-107019>. ↵
12. Washington Laws of 2026, Chapter 239, Engrossed Substitute Senate Bill 6002, <https://lawfilesextra.leg.wa.gov/biennium/2025-26/Pdf/Bills/Session%20Laws/Senate/6002-S.SL.pdf>. ↵
13. Oregon Laws 2026, Chapter 77, https://www.oregonlegislature.gov/bills_laws/lawsstatutes/2026orLaw0077.pdf. ↵
14. New Mexico Laws of 2026, Chapter 20, Senate Bill 40, Driver Privacy and Safety Act (effective July 1, 2026), final text: <https://www.nmlegis.gov/Sessions/26%20Regular/final/SB0040.pdf>. ↵
15. Utah Code Sections 41-6a-2003 through 41-6a-2005 (nine-month retention limit at Section 41-6a-2004), https://leg.utah.gov/xcode/Title41/Chapter6A/C41-6a-P20_1800010118000101.pdf; Utah Office of Data Privacy, "25-04 Automatic License Plate Readers," <https://privacy.utah.gov/25-04-automatic-license-plate-readers/>. ↵
16. U.S. Constitution Annotated, "Anti-Commandeering Doctrine," Library of Congress, https://constitution.congress.gov/browse/essay/amdt10-4-2/ALDE_00013627/; *Murphy v. National Collegiate Athletic Association*, 584 U.S. 453 (2018). ↵
17. *Chatrpie*, supra note 3. ↵
18. Washington Laws of 2026, Chapter 239, Section 3(6); Oregon Laws 2026, Chapter 77, Section 4(6). ↵

19. Oregon Laws 2026, Chapter 77, Section 4(3); Washington Laws of 2026, Chapter 239, Section 4; Flock Safety, "How Flock Protects and Manages Data," vendor statement, <https://www.flocksafety.com/trust/data-privacy>. ↩
20. Utah Code Section 41-6a-2005. ↩
21. Washington Laws of 2026, Chapter 239, Section 3(3)-(4). ↩
22. Washington Laws of 2026, Chapter 239, Section 5(6)-(8). ↩
23. New Mexico Laws of 2026, Chapter 20, Section 3(E); Washington Laws of 2026, Chapter 239, Section 5(4). ↩
24. The Verge, *supra* note 8. Flock described the issue as a limited misconfiguration that had been remedied. ↩
25. Oregon Laws 2026, Chapter 77, Section 9; New Mexico Laws of 2026, Chapter 20, Section 5. ↩
26. Utah Code Section 41-6a-2003(3); Washington Laws of 2026, Chapter 239, Section 7. ↩
27. Washington Laws of 2026, Chapter 239, Section 7(2). ↩
28. GAO-25-107019, *supra* note 11. ↩
29. U.S. Constitution Annotated and *Murphy*, *supra* note 16. ↩
30. Associated Press, *supra* note 5; KPRC 2, *supra* note 6; ABC7 San Francisco, *supra* note 7. ↩