REKOR SYSTEMS

ALPR AND PRIVACY

A practical framework for preserving public-safety value while reducing unnecessary privacy risk

Prepared for citizens, policymakers, public-safety leaders, civil-rights stakeholders, technology partners and OEMs

July 2026

Executive Summary

Automated license plate recognition (ALPR) and vehicle recognition technologies have demonstrated their critical role in public safety for many years. They help agencies identify stolen vehicles, locate wanted vehicles, respond to Amber and Silver Alerts, support investigations, and protect critical infrastructure. At the same time, there has been a growing backlash against ALPR. The controversy has moved from privacy-policy circles into city councils, litigation, mainstream news, and viral online discussion.

Much of the recent backlash has been associated with Flock Safety. Public reporting, lawsuits, and advocacy campaigns involving Flock have made the company a shorthand for the broader surveillance-state concern: ordinary drivers do not want their daily movements collected, stored, searched, shared, or exposed when there is no public-safety reason to identify them.

Rekor believes this debate need not be all-or-nothing. The future of vehicle recognition should be governed by privacy-by-architecture: anonymizing vehicles that are not on a duly authorized hotlist by default, retaining identifiable records only when policy and lawful purpose justify it, and ensuring the underlying video evidence can be proven authentic when it matters.

This paper outlines a three-part architecture that Rekor believes can help bring the two sides of this national debate together. It is intended as a discussion framework for policymakers, civil rights stakeholders, public safety leaders, technology partners, OEMs, and industry participants to consider how vehicle recognition should operate in a more regulated environment.

Purpose of This Paper

This white paper is intended to describe a workable policy and technology framework in plain language. The goal is to help define how vehicle recognition systems can preserve legitimate public-safety value while reducing unnecessary privacy risk and improving evidentiary trust. It is organized around outcomes that a responsible framework can achieve with available technology: protecting the privacy of non-relevant data, purpose-based retention, auditable access, customer and community control, and evidence integrity.

Although much of the controversy has focused on Flock Safety, it should not obscure the larger point: the issue is industry-wide, and a responsible framework should apply to all ALPR and vehicle recognition systems.

The Problem: The Flock Backlash and the Surveillance-State Concern

Vehicle recognition has legitimate public-safety value. Agencies use ALPR to locate stolen vehicles, vehicles associated with missing-persons alerts and past criminal activities, and vehicles connected to active investigations. For many agencies, the technology has become part of the practical toolkit for public safety.

The concern is not that vehicle recognition has no value. The concern is that many legacy systems can treat every plate read the same way: collect it, identify it, retain it, share it, and make it searchable. That model can create large location databases involving ordinary drivers who are not suspected of wrongdoing.

The Flock controversy has accelerated the conversation by providing the public with a concrete example. Whether the discussion is about unauthorized or unexpected data sharing, federal access, retention, accuracy, misuse, hacking fears, litigation, or community consent, the underlying question is the same: who controls the data, what happens to the vast amount of Personally Identifiable Information ("PII") data collected about ordinary drivers, and what proof exists when evidence is challenged?

A better framework distinguishes among three categories of data: ordinary (non-hit) observations, authorized public-safety alerts, and records that become evidence when policy and lawful purpose justify retention. Rekor's architecture is built around that distinction.

Rekor's Three-Part Architecture

1. Non-Hit Anonymization

Rekor's first pillar is our patented technology for protecting personal identification data in vehicle recognition systems, including license plate recognition. The architecture is designed to support obfuscation, encoding, or anonymization of vehicle-identification data at the point of collection while preserving operational value.

This is the central privacy bridge. A vehicle that is not on a hotlist, wanted list, Amber or Silver Alert list, or any other legally authorized investigative list should not be treated like a vehicle connected to a public-safety event. Non-hit data can be protected differently from authorized hits.

- Policy implication: ALPR systems do not need to choose between deleting everything and retaining everything. The architecture can support operational use while reducing the unnecessary exposure of ordinary, non-suspect vehicle data.

2. Policy-Based Evidence Retention

Rekor's second pillar is technology we have developed for policy-centric data retention. Traditional ALPR policies often rely on fixed time periods, such as 30, 60, or 90 days, regardless of whether the record is tied to a stolen vehicle, a violent felony, a missing person, or no public-safety event at all.

A policy-based retention model ties retention to factors such as hotlist match, offense severity, investigatory relevance, agency policy, legal requirements, and community expectations. The purpose is to preserve what matters while reducing the scope and duration of unnecessary identifiable records.

- Policy implication: Retention should be purpose-based, not merely time-based. Communities can set rules that reflect public-safety need, civil-liberties risk, and legal requirements.

3. Go-Secure.Video Authenticated Media Capture

Rekor's third pillar is Go-Secure.Video, a patent-pending media-authentication technology designed to verify video integrity from the moment of capture. Go-Secure.Video addresses a different but related issue: evidence trust.

Even if a system handles privacy correctly, agencies, courts, insurers, journalists, enterprises, and the public still need to know whether the underlying video has been altered, truncated, or spliced. Go-Secure.Video is designed to authenticate media at or near capture and support later validation when the original media is produced.

- Policy implication: Responsible vehicle recognition should not only govern data collection and retention; it should also support evidence-grade integrity for the video and image records that may be used in investigations, insurance claims, disputes, litigation, journalism, and public accountability.

The Regulatory Compromise

A workable regulatory scheme does not need to eliminate vehicle recognition. It can require better architecture. The question should not be whether ALPR exists. The question should be: how is ALPR designed, governed, audited, and limited?

A privacy-first framework could require that systems:

- Protect non-hit data by default, including through anonymization, encoding, or other privacy-protective treatment.
- Allow authorized hotlist, wanted-vehicle, missing-person, and legally approved investigative uses.
- Apply retention policies based on lawful purpose, offense severity, investigatory relevance, and community-approved rules.
- Maintain auditable access logs showing who accessed data, when, and for what stated purpose.
- Verify the integrity of video evidence used to support alerts, investigations, claims, or litigation.
- Support existing infrastructure and OEM ecosystems so agencies can modernize without unnecessary hardware replacement.

Why This Matters to Public Safety

Public safety agencies need tools that work. A stolen vehicle, wanted vehicle, Amber Alert, Silver Alert, or credible threat should still be actionable. A responsible architecture should preserve those capabilities while reducing the unnecessary retention and exposure of ordinary driver data.

This approach allows agencies to explain better their deployments: the system is not designed to build a broad, indefinite location database of ordinary drivers. It is designed to respond to predefined public-safety events, protect non-relevant data, retain evidence in accordance with policy, and verify video integrity when needed.

Why This Matters to Civil Liberties

Civil-liberties concerns are not a public-relations problem; they are an architecture problem. If a system collects identifiable location data from every vehicle and retains it broadly, the public will reasonably ask how that data can be searched, shared, breached, misused, or requested through legal process.

The anonymization of non-relevant data and policy-based retention of relevant data provide a way to address public concerns. They allow communities to ask specific questions: What happens to ordinary non-relevant data? What gets retained? For how long? Who can access it? Under what legal standard? Can the video evidence be proven to be authentic?

Why This Matters to Industry Participants and OEMs

The market opportunity is not limited to selling cameras or recognition software. The larger opportunity is to define the trusted architecture for regulated vehicle recognition. Vendors that can demonstrate privacy-by-design and evidence-grade integrity may be better positioned with agencies, regulators, communities, and enterprise customers.

As concerns about the use of ALPR systems spread, system providers and operators will face increasing pressure to demonstrate privacy protection, lawful access controls, policy-based retention, auditability, and evidence integrity. Rekor believes these requirements will become core buying criteria rather than optional features.

Rekor's goal is to help move the market beyond the current fight. If lawmakers, agencies, and civil rights stakeholders can agree on measurable outcomes, the industry can compete to achieve them while preserving legitimate public-safety value.

Implementation Considerations

- Technology standards should be measurable. A system should be able to demonstrate how non-relevant data is protected, how retention policies are applied, how access is audited, and how evidence integrity is verified.
- Policies should be configurable and enforceable. Agencies should be able to set policies that reflect legal requirements and community expectations, but those policies should be implemented in the technology, not left entirely to manual practice.
- The architecture should support existing infrastructure. Agencies and OEMs should not have to replace every camera, storage environment, or workflow to adopt privacy and evidence safeguards.
- Regulation should be technology-neutral but outcome-specific. Lawmakers do not need to mandate one vendor. They can require outcomes such as non-hit protection, limited access, purpose-based retention, audit logs, and media integrity verification.

Discussion Questions

- Should non-hit plate data be anonymized or encoded by default?
- What categories of public-safety events should justify retention of identifiable data?
- How should communities participate in setting retention and access policies?
- What audit rights should agencies, oversight bodies, and the public have?
- Should evidentiary video be required to include cryptographic integrity verification?
- How can privacy requirements be implemented without eliminating legitimate public-safety uses?

Conclusion

A false choice between public safety and civil liberties should not define the next phase of vehicle recognition. It should be defined by architecture: what is captured, what is protected, what is retained, who can access it, and whether the evidence can be proven.

The public attention focused on Flock cameras has made the issue national. Rekor believes that is not a reason to abandon vehicle recognition. It is a reason to rebuild the discussion around privacy-by-design, purpose-based retention, auditable access, and evidence integrity.

Protect non-hit data. Retain only what policy justifies. Prove the evidence when it matters. That is the foundation for responsible vehicle recognition in a regulated environment.

Public Reporting, Litigation, and Advocacy Timeline

The following public sources are included to illustrate the speed and breadth of the national ALPR debate and the nature of the concerns expressed. They are listed in date order, with the most recent items first. Allegations in lawsuits and reporting are allegations unless and until resolved by the appropriate court or public authority.

Date	Source	Item	Link
July 2, 2026	ACLU	Flock Safety Credibility Lost as it Repeatedly Lies to City Councils, Police Departments, and Public Across the Country	link
June 29, 2026	TechTimes	Flock Safety Crosses 100,000 Cameras as 53 Cities Cancel Over Unauthorized Federal Data Access	link
June 29, 2026	ACLU	How to Fight Deployment of Flock and Other Mass Surveillance License Plate Readers in Your Community	link
June 27, 2026	The Wall Street Journal	The Nationwide Backlash Against Cameras Watching Your Car	link
June 2026	404 Media	Cops Keep Getting Arrested for Using Flock to Stalk People	link
June 2026	404 Media	Flock Leaked Cops' License Plate Searches via DuckDuckGo, Bing	link

June 2026	Business Insider	There's a trash-bag revolt brewing against Flock license plate readers	link
June 8, 2026	Freedom's Phoenix	How to Get Flock Cameras Out of Your Community	link
May 1, 2026	ClassAction.org	Class Action Lawsuit Alleges Home Depot Parking Lot Cameras Secretly Transmit Driver Data to Law Enforcement	link
April 20, 2026	ACLU / EFF	Schmidt v. Norfolk amicus challenging Norfolk use of Flock ALPRs	link
April 15, 2026	Institute for Justice / San Jose	San Jose ALPR federal class-action challenge involving Flock cameras	link
April 6, 2026	The Guardian	Creepy surveillance: why some cities are shutting down Flock cameras amid privacy concerns	link
April 3, 2026	Gibbs Mura / Flock class action	Amended class action complaint against Flock alleging California ALPR privacy violations	link
April 2, 2026	arXiv	Street-Legal Physical-World Adversarial Rim for License Plates	link
March 26, 2026	404 Media	Police Used Flock to Give a Man a Traffic Ticket	link
March 2026	Business Insider	AI cameras are everywhere - and people are paying the price for their mistakes	link
February 27, 2026	BusinessWire / Gibbs Mura	Flock License Plate Cameras Face Class-Action Lawsuit	link
February 23, 2026	TechCrunch	Americans are destroying Flock surveillance cameras	link
February 20, 2026	Carscoops	Why More Cities Are Suddenly Pulling The Plug On Flock Safety Cameras	link
February 17, 2026	NPR / KNAU	Why some cities are ditching their Flock license plate readers	link
January 2026	ACLU	Automatic License Plate Reader Privacy Model Bill	link
January 2026	Ars Technica	Norfolk residents lose lawsuit to stop Flock license plate scanners	link
December 2025	EFF	EFF's investigations expose Flock Safety surveillance abuses: 2025 in review	link
November 2025	EFF	Washington court rules data captured by Flock Safety cameras are public records	link
August 18, 2025	ACLU	Flock's Aggressive Expansions Go Far Beyond Simple Driver Surveillance	link
June 2025	EFF	Victory! Austin Organizers Cancel City's Flock ALPR Contract	link

Rekor Intellectual Property and Product References

The following Rekor intellectual-property and product references are included for context. These descriptions are for policy and business discussion only and are not a legal claim construction or legal opinion.

- Rekor Systems: Rekor Systems Offers Policymakers a Privacy-Protected and Responsible Path Forward for the Use of Automated License Plate Recognition. link
- Rekor Systems: Rekor Systems Secures Landmark Patent for Incident-Based Data Retention, Replacing Outdated ALPR and Vehicle Dragnets with Privacy-First Intelligent Storage. link
- USPTO Official Gazette: U.S. Patent No. 11,983,294, issued May 14, 2024. link
- Google Patents: U.S. Patent No. 12,548,437, Systems and methods for policy-centric data retention in traffic monitoring, issued February 10, 2026. link
- Rekor Systems: Rekor Systems Launches Rekor Scout Axis Agent With Go-Secure.Video. https://www.rekor.ai/post/rekor-systems-launches-rekor-scout-axis-agent-with-go-secure-video-bringing-trusted-and-tamper-evident-video-to-standard-axis-cameras
- Rekor Systems: Rekor Introduces Go-Secure.Video: Proof That Video Is Real. https://www.rekor.ai/post/rekor-introduces-go-secure-video-proof-that-video-is-real