



Legislative Policy Framework: Automated License Plate Reader (ALPR) Systems

October 7, 2026

California Police Chiefs Association

Peace Officers Research Association of California

California State Sheriffs' Association

OVERVIEW OF ALPR:

Automated License Plate Reader (ALPR) technology has become an increasingly important tool for California law enforcement, helping officers identify stolen and wanted vehicles, locate missing and endangered persons, develop investigative leads, and more quickly connect vehicles to serious crimes. The technology can produce meaningful public safety results. At the same time, the effectiveness of ALPR depends on public confidence that the enormous volume of information collected by these systems will be accessed only for legitimate law enforcement purposes and protected against misuse, unauthorized sharing, and improper access. California law already recognizes this balance by regulating the collection, use, storage, and sharing of ALPR information. This 2027 Policy Framework seeks to build on those protections by establishing clear and enforceable standards for training, accountability, transparency, privacy and data security, and vendor compliance—while preserving law enforcement’s ability to use ALPR technology responsibly as an effective investigative and public safety tool.

EXISTING CALIFORNIA FRAMEWORK:

Civil Code §§ 1798.90.5-1798.90.55 (SB 34, 2015) already regulates ALPR operators and end-users. Existing law requires security safeguards; written, publicly available usage/privacy policies; identification of authorized uses and users; training requirements; monitoring and periodic audits; retention rules; access logs recording date/time, query, username and purpose; and limits public agencies to sharing ALPR information with another California public agency as otherwise permitted by law. It also provides a civil remedy for knowing violations and requires public comment before a public agency implements an ALPR program.

DOJ guidance and related California protections. In 2023, DOJ issued ALPR guidance and a model policy interpreting civil codes above to prohibit California law enforcement agencies from sharing ALPR information with federal or out-of-state agencies, including through vendor-hosted databases. DOJ has since pursued enforcement of that interpretation. Separate California laws also restrict law enforcement cooperation or information sharing for civil immigration enforcement and for investigations arising from reproductive or gender-affirming health care that is lawful in California. The 2027 framework should build on these existing protections rather than recreating them.

Key authorities: Civ. Code §§ 1798.90.5-.55; DOJ Information Bulletin 2023-DLE-06 and DOJ General Order 2023-05; California Values Act (Gov. Code § 7284 et seq.); Pen. Code § 13778.2 (lawful reproductive care); related California shield-law protections for lawful gender-affirming care.

COMPREHENSIVE LEGISLATIVE FRAMEWORK

1. Training & Certification

- **Statewide certification prerequisite.** ALPR access requires a unique certification number issued only after successful completion of POST-approved training and a written examination. No certification number means no system login.
- **Annual recertification.** Certification must be renewed annually; expired or failed certification automatically suspends system access until requirements are satisfied.

- **Core curriculum.** Training must cover authorized and prohibited uses, privacy and ethics, applicable California and federal law, data-sharing restrictions, documentation requirements, and the administrative, civil, and criminal consequences of misuse.
- **Individual accountability.** Certification and credentials are assigned to the individual user and may not be shared, transferred, or used through generic/group accounts.

2. Oversight & Accountability

- **Random DOJ audits.** Authorize DOJ to conduct randomized compliance audits of state and local agencies using ALPR, including review of policies, user certifications, searches, sharing settings, vendor configurations, and audit logs.
- **Agency-level review.** Require periodic internal audits designed to identify anomalous searches, missing case/reason fields, unauthorized sharing, and access by uncertified users.
- **Criminal misuse.** Establish a targeted criminal offense for a peace officer or other authorized user who knowingly accesses or uses ALPR information for an unauthorized personal, commercial, discriminatory, retaliatory, or other non-law-enforcement purpose. Penalties should focus on intentional misuse rather than good-faith mistakes.
- **Corrective action.** Material violations trigger access suspension, investigation, remediation, and preservation of relevant logs; existing disciplinary and civil remedies remain available.

3. Transparency

- **Public ALPR webpage.** Every agency using ALPR must maintain a clearly accessible ALPR transparency webpage controlled by the agency.
- **Minimum disclosures.** The page should identify the agency's ALPR policy, purpose and authorized uses, camera/system deployment information at an appropriate level of detail, data-retention period, categories of agencies with which data may be shared, vendor(s), current sharing status, and contact information for questions or complaints.
- **Aggregate usage reporting.** Publish periodic, non-case-specific statistics such as total searches, number of cameras or data sources, audit activity, and confirmed policy violations, while protecting active investigations, investigative methods, victim information, and officer safety. Agencies may also include crime statistics or clearance rates involving ALPR systems.
- **Current information.** Agencies must update the webpage when material policies, vendors, retention periods, or sharing configurations change.

4. Privacy & Data Protection

- **Mandatory search documentation.** Each search must record the case/incident number (or other authorized event identifier), a brief but sufficiently detailed law enforcement reason, the officer/user name and certification-linked credential, and the date and time.
- **Purpose limitation.** ALPR information may be accessed only for an authorized law enforcement purpose and consistent with existing California restrictions on immigration enforcement, reproductive care, gender-affirming care, and other protected activity.
- **Historical-data safeguard.** For ALPR data older than 12 months, require a specialized California court order when the search is not tied to an ongoing investigation. The application must establish probable cause or reasonable suspicion, as specified by statute, and identify the investigative purpose and scope of the requested historical search.
- **Data minimization and security.** Require reasonable retention limits established at the local level, strong authentication, encryption and security controls, preservation when required for evidence, and auditable deletion consistent with law and agency policy.

5. Vendor Compliance & Enforcement

- **California-by-default architecture.** California ALPR data remains in the ownership of each law enforcement agency and must remain in California unless the contracting agency gives explicit written authorization for a specific, legally permissible request. No default national lookup, silent statewide sharing, or built-in federal/out-of-state query access.

- **Visible compliance controls.** Vendors must configure products to comply with California law through settings the contracting agency can view, control, and audit. Material product or sharing-setting changes must not silently expand access.
- **Certification-linked credentials and complete logs.** Unique user credentials must be tied to the user's certification number. The vendor must maintain a complete, unredacted audit log available to the contracting agency showing user, date/time, plate or query, stated reason, and case/incident number.
- **48-hour incident notice.** A vendor that discovers a misconfigured share, unauthorized outside access, or other material compliance failure must notify the affected contracting agency within 48 hours of known incident and preserve relevant records.
- **Prohibited vendor conduct.** Selling California plate data, knowingly enabling an unlawful recipient to obtain it, or conducting a "side-door" search on behalf of an agency that could not lawfully receive or query the data constitutes a violation.
- **Enforcement standard and remedies.** Apply liability where the vendor knowingly or through gross negligence violates these requirements. Authorize civil penalties up to \$15,000 per violation plus proven damages and appropriate equitable relief.
- **Local and state enforcement.** A local agency or district attorney with a vendor contract may bring an action for violations involving that agency's data or system. DOJ and the appropriate state administrative authority may enforce violations involving state agencies, statewide systems, or DOJ.

Policy Principle

The framework should distinguish between misuse by an individual user, agency compliance failures, and vendor/system failures. Rules should be technologically enforceable wherever possible, with access controls and auditability built into the product, while preserving legitimate investigative use, interagency cooperation permitted by California law, and due process protections before criminal or civil liability attaches.