Summary of Proposed Amendments to S.B. 1111

Automated License Plate Readers — Privacy Protections & Citizen Oversight

Fifty-seventh Legislature, Second Regular Session

Overview

S.B. 1111, as adopted by the Senate Committee on Appropriations, Transportation and Technology, authorizes law enforcement agencies across Arizona to use Automated License Plate Reader (ALPR) systems. While the adopted version includes some basic requirements — training, password-protected access, case number tracking — it lacks meaningful guardrails against mass surveillance, indefinite data retention, and abuse. It also entirely ignores the widespread use of ALPR cameras by homeowners associations and school districts through vendors like Flock Safety.

These amendments transform S.B. 1111 from one of the weakest ALPR bills in the country into one of the strongest. The approach is practical: **law enforcement gets a reasonable 30-day window to use plate data for legitimate investigations, but every query into stored data requires a documented felony case number, supervisor sign-off, and a full audit trail. No more browsing. No more fishing expeditions. No more indefinite storage.**

Below is a plain-language explanation of each change.

Changes to Definitions (§28-1241)

Closes the "Official Purposes" Loophole

What the original says: Official law enforcement purposes "includes" a list of uses.

The problem: In Arizona law, "includes" means "includes but is not limited to." Agencies could claim virtually anything qualifies.

What the amendment does: Changes "includes" to "means only the following" and lists the specific authorized purposes. If it's not on the list, it's not allowed.

Tightens the Watchlist Definition

Removes the catch-all "other active criminal investigations" language. Watchlists are limited to stolen vehicles, felony warrants, missing/endangered persons, AMBER/Silver Alerts, and human trafficking. Explicitly excludes general intelligence gathering and predictive policing.

Covers Reverse Location ("Geofence") Queries

Expands the definition of "aggregation" to cover queries like "show me every car at 5th and Main last Tuesday." These geofence-style searches now require a warrant.

Defines "Vendor" and "Homeowners Association"

Adds definitions for “vendor” (any company like Flock Safety that provides or stores data for ALPR systems) and “homeowners association.” This allows the bill to regulate these entities directly.

Changes to Allowable Uses (§28-1242)

Narrows “Patrol Operation” to Require a Case Number

The original allowed ALPR use “in conjunction with any patrol operation,” which effectively authorized blanket scanning at all times. The amendment requires a documented case number for a felony offense or one of the specifically listed purposes.

Adds Explicitly Prohibited Uses

ALPRs may not be used for: civil asset forfeiture, immigration enforcement, enforcement of non-criminal offenses, or monitoring/tracking individuals based on race, ethnicity, religion, political affiliation, or exercise of First Amendment rights including protest attendance.

Makes Verification Mandatory, Not Optional

The original said officers should verify alerts “if practicable.” The amendment makes verification mandatory: a match alone is not reasonable suspicion. Officers must visually confirm the plate and verify through dispatch or NCIC before making a stop.

Restricts Camera Capabilities

Cameras must read plates only. They cannot photograph vehicle occupants. This prevents mission creep into general surveillance.

Changes to Data Collection Rules (§28-1243)

Removes the Blanket Public Records Exemption

The original exempted all ALPR data from public records requests. The amendment replaces this with a transparency framework — agency policies, audit logs, usage statistics, disciplinary records, and reports are all public records.

Upgrades Misuse from Misdemeanor to Felony

Tiered penalties: unauthorized access is a Class 6 felony; stalking/tracking is a Class 5 felony; selling data is a Class 5 felony; reckless misuse is a Class 1 misdemeanor. Anyone convicted is permanently banned from accessing any ALPR system in Arizona.

Adds an Exclusionary Rule

ALPR data obtained in violation of this article — and any evidence derived from it — is inadmissible in any proceeding. This prevents agencies from violating the rules, accepting the penalty, and still using the evidence.

Bans Sharing with Federal Agencies and Out-of-State Entities

Arizona ALPR data cannot be shared with any federal agency (including ICE), any out-of-state agency, any private entity, or any vendor-operated data network — except by warrant from an Arizona court.

Data Retention — The Core Reform (§28-1244)

The approach: Law enforcement gets a practical 30-day retention window. This addresses legitimate needs — a missing person may not be reported for days, a vehicle linked to a crime scene may not be identified immediately. But storing data and accessing data are two different things. The guardrails are on ***access***, not just deletion.

30-Day Maximum Retention — Hard Deadline, Automatic Destruction

All captured plate data is automatically and permanently destroyed after 30 days. It cannot be archived, backed up, or transferred to any system that would allow retention beyond 30 days without a warrant.

Two Tiers of Access During the 30-Day Window

Tier 1 — Real-time alerts (no additional authorization): When a plate triggers a match against an active watchlist in real time, the on-duty officer can immediately access the alert to verify it and respond. This is the normal operational use case.

Tier 2 — Retroactive investigative queries (supervisor approval required): If an investigator wants to go back and search stored data — "was this plate seen anywhere in the last two weeks?" — they must have: (a) a documented felony case number, (b) written approval from a supervisor of sergeant rank or above specifying the case number, plate number or area, time period, and factual basis for the query, and (c) full logging of the query, the approval, and the results in the audit trail. No browsing. No curiosity searches. No supervisor approval, no access.

What Doesn't Count as Lawful Access

The amendment explicitly lists what is *not* a valid reason to query stored data: browsing without a case number, non-felony offenses, general incident numbers, traffic citations, civil matters, or the claim that data "might be useful someday." Monitoring or tracking anyone who is not a named suspect in a documented felony is also prohibited.

Warrant Required Beyond 30 Days — Hard Cap at 1 Year

To keep data past 30 days, a judge must issue a warrant based on probable cause specifying the exact plates, investigation, and a retention period of no more than 90 days. Renewals are limited to 3 times, and each requires proof the prior retention produced evidence. Absolute maximum: 1 year from capture, no exceptions.

No Bulk Databases

No agency, vendor, or any other entity may maintain a database of ALPR data beyond the authorized retention periods. Bulk collection and indefinite storage of plate data is prohibited.

Warrant Required for Aggregation, Profiling & Geofence Queries (§28-1245)

Building movement histories, pattern-of-life analyses, or running “show me every car at this location” queries all require a warrant with specific particularity requirements. This ensures ALPR data is used to investigate specific crimes, not to conduct dragnet surveillance.

Watchlist Governance (§28-1246)

Every watchlist entry requires a documented law enforcement basis and supervisor approval (sergeant or above). Entries auto-expire after 90 days unless renewed. Bulk-loading plates is prohibited. The AG can audit the watchlist. Monthly reporting of all watchlist activity is required.

Vendor Obligations (§28-1247)

Companies like Flock Safety are bound to every restriction in the bill. They cannot retain copies of Arizona data beyond 30 days, cannot combine it with data from other states, cannot sell or share it, and cannot use it to build commercial products. Contracts must include compliance requirements, quarterly destruction certifications, and AG audit provisions. Violations are felonies and grounds for contract termination.

Warrant Required for Police Access to Private ALPR Systems (§28-1248)

Police need a warrant to access any private ALPR system — whether owned by an HOA, a business, or a vendor — regardless of how the access occurs (electronic, written, or verbal). Standing agreements for ongoing access without individual warrants are prohibited. Private entities that voluntarily share data with police without a warrant face $5,000–$50,000 civil penalties per violation.

Homeowners Association ALPR Requirements (§28-1249)

Why this matters: Flock Safety has aggressively marketed ALPR cameras to HOAs across Arizona. These cameras scan every plate entering and leaving a community, and the data is stored on Flock’s cloud. In many cases, HOA boards approved these systems without a homeowner vote and without disclosing that data may be shared with police or retained indefinitely. The original S.B. 1111 doesn’t address this.

What the amendment does: Majority homeowner vote required before deploying cameras. 30-day data retention limit. No sharing with police or anyone else without a warrant. Security-only use. Signage at all entrances. Written data policy for members. Residents can request and delete their own data (10-day response). Vendor contracts must prohibit warrantless sharing, aggregation, and retention past 30 days. $5K–$50K civil penalties. AG enforcement authority.

School District ALPR Requirements (§28-1250)

Why this matters: ALPR cameras at schools scan every parent, staff member, and visitor during drop-off and pick-up. When stored in the cloud, this data reveals detailed family routines. Federal law (FERPA) may apply to plate data that can identify students or their families.

What the amendment does: Public board vote with 30 days' notice to parents. Campus security use only. Cameras cannot photograph occupants. 30-day retention, warrant-only sharing. Cannot be used to monitor/track/discipline students or families. Plate data that identifies students treated as FERPA student records. Same vendor contract restrictions. $5K–$50K civil penalties. AG enforcement authority.

Local Control — Citizens Can Veto Surveillance (§28-1251)

Cities, towns, and counties can ban ALPRs. If they do, no other agency — including MCSO, DPS, or any state agency — can deploy cameras within that community. The only exception is mobile readers on interstate highways (not state routes or local roads), capped at pre-ban levels.

Transparency Portal & Citizen Data Access (§28-1252)

Public online portal showing: camera locations, plates scanned, matches, retroactive queries conducted, stops/arrests, errors/breaches, and every entity the agency shared data with (date, purpose, legal authority). Residents can request their own data (15-day response), request deletion (10 days), and agencies can only withhold data for an active investigation for up to 1 year.

Mandatory Reporting & AG Oversight (§28-1253)

Monthly reports to the AG covering all system activity including retroactive queries and their case numbers. Automatic ALPR shutdown if reports are 30+ days late. Mandatory annual AG audit of every agency (including vendor systems and watchlists). Annual statewide summary to legislative leadership and the Governor, posted publicly.

Your Right to Your Own Data (§28-1254)

Every Arizonan can obtain all ALPR data about their own vehicle — images, dates, locations, who accessed it, who it was shared with. Free first request per year. Cannot be denied on exemption grounds.

Citizens Can Sue (§28-1255)

Any violation — by police, an HOA, a school, a vendor, or anyone — gives the affected person standing to sue for actual damages, $2,500+ statutory damages per violation, attorney fees, and injunctive relief. Sovereign and qualified immunity waived.

3-Year Sunset (§28-1256)

Entire article repealed January 1, 2029. Legislature must vote to reauthorize as AI and surveillance technology evolves.

The Bottom Line

These amendments don't take tools away from law enforcement. Police get 30 days of stored data and can query it for any documented felony investigation with supervisor approval. What the amendments eliminate is the ability to browse that data without justification, store it indefinitely, share it with the feds or out-of-state agencies, let vendors build national tracking databases, or override a community's decision to say no. Every query is logged. Every access has a name attached. Every violation has teeth.

In short: **30 days of data with real accountability beats unlimited data with no accountability.**