Arizona Senate Fact Sheet Proposed Amendments to S.B. 1111 *(written by citizens)* Automated License Plate Readers - Privacy Protections & Citizen Oversight.

Visit whattheflock.us for more information.

The Problem

The current version of S.B. 1111 authorizes statewide ALPR use by law enforcement but provides only minimal safeguards: basic training, password access, and case tracking. It contains no limits on indefinite data retention, no restrictions on mass surveillance or "fishing expeditions," no rules for private vendors (e.g., Flock Safety), and no oversight for HOAs or schools. Arizona risks becoming one of the weakest ALPR states—creating a permanent dragnet surveillance system with no real accountability.

The Solution

These amendments turn S.B. 1111 into one of the strongest ALPR bills in the country while preserving legitimate law-enforcement tools. Core bargain: Law enforcement gets a practical 30-day window for real-time alerts and documented felony investigations. In exchange, every query requires a felony case number + supervisor sign-off, data is automatically destroyed after 30 days, and citizens gain transparency and enforcement rights.

Key Amendments by Priority Tier

Tier 1 — Structural Essentials (prevent mass surveillance architecture)

- Closed "official purposes" list (limited to stolen vehicles, missing persons, human trafficking, felony warrants, crime scenes)
- Prohibited uses (no civil forfeiture, immigration, non-criminal enforcement, or tracking based on race/religion/politics/First Amendment)
- 30-day hard retention + auto-destruction (no backups/archiving without warrant)
- Retroactive queries require felony case # + sergeant+ approval + audit log (no browsing)
- Exclusionary rule (violative data/evidence inadmissible)
- Vendor rules (Flock bound by same limits; no parallel database

Tier 2 — Closing Backdoors

- Warrant required for private ALPR access (HOAs, businesses, vendors)
- No federal/out-of-state sharing without AZ warrant
- Strict watchlist & aggregation/geofence rules (warrant for profiling/reverse queries)

Tier 3 — Accountability & Transparency

- Felony penalties for misuse + permanent ALPR ban
- Mandatory AG reports/audits + public portal (locations, usage stats)

Tier 4 — Citizen & Private Entity Protections

- HOA/school rules (vote required, 30-day retention, resident data access/deletion)
- Right to your data + deletion requests

- Private right of action ($2,500+ damages, fees)

Tier 5 — Long-Term Safeguards

- Local bans allowed (no state override)
- 3-year sunset (re-review in 2029)

Bottom Line for Legislators

- Law enforcement still wins: 30 days of data + real-time alerts for stolen cars, missing kids, felony warrants.
- Citizens win: No indefinite tracking databases, no warrantless sharing with feds or vendors, local communities can ban ALPRs, and every misuse has real penalties.

Vote YES on these amendments. They deliver targeted public safety without creating a permanent surveillance infrastructure, which can lead to 15-minute city digital prisons (Oxford, England) or draconian lock downs (China & Australia).

30 days of accountable data beats unlimited data with no accountability.

Citizen Contact: Merissa Caldwell, 480-374-0102, merissa@merissacaldwell.com