S.B. 1111 Amendment Priority Framework

25 Amendments Ranked by Structural Importance

Privacy • Anti–Mass Surveillance • Anti–15-Minute City Infrastructure

Fifty-seventh Legislature, Second Regular Session

How to Read This Document

Each amendment shows its priority rank, strategic description, and actual proposed statutory language. Tier 1 = structural essentials. Tier 2 = closes backdoors. Tiers 3–5 = accountability, citizen rights, and safeguards. If negotiating, protect Tiers 1–2 before conceding anything in Tiers 3–5.

Amendments marked **● ANTI-15-MIN CITY** are the five provisions most critical for preventing ALPR infrastructure from being repurposed for zone-based movement enforcement — the surveillance backbone of 15-minute city enforcement as implemented in Oxford, England.

The green-bordered ***Amendment Language*** sections contain the actual proposed statutory text.

TIER 1 — THE STRUCTURAL ESSENTIALS

Without these, passing S.B. 1111 is worse than not passing it at all. These provisions prevent the bill from legalizing a mass surveillance architecture with no meaningful limits.

#1 Prohibited Uses List (§28-1242(B)) ● ANTI-15-MIN CITY

Prohibits ALPRs for non-criminal enforcement, civil asset forfeiture, immigration enforcement, and monitoring based on race, religion, political affiliation, or First Amendment activity. This is the single most important amendment — it prevents ALPR infrastructure from being repurposed for zone-based enforcement, congestion pricing, travel allowances, or protest tracking. The Oxford model of 15-minute city enforcement depends entirely on using plate readers for civil/administrative violations. This amendment makes that illegal in Arizona.

Amendment Language:

B. AN AUTOMATED LICENSE PLATE READER SHALL NOT BE USED FOR ANY OF THE FOLLOWING PURPOSES:

1. CIVIL ASSET FORFEITURE PROCEEDINGS.
2. IMMIGRATION ENFORCEMENT OR THE ENFORCEMENT OF ANY FEDERAL CIVIL IMMIGRATION LAW.
3. THE ENFORCEMENT OF ANY OFFENSE THAT IS NOT A CRIMINAL OFFENSE UNDER THE LAWS OF THIS STATE.
4. THE MONITORING, TRACKING OR SURVEILLANCE OF ANY INDIVIDUAL BASED ON THAT INDIVIDUAL'S RACE, ETHNICITY, NATIONAL ORIGIN, RELIGION, GENDER, SEXUAL ORIENTATION, POLITICAL AFFILIATION, EXERCISE OF RIGHTS PROTECTED UNDER THE FIRST AMENDMENT TO THE UNITED STATES CONSTITUTION, OR PARTICIPATION IN LAWFUL PROTEST OR ASSEMBLY.

#2 Vendor Obligations (§28-1247) ● ANTI-15-MIN CITY

Binds vendors like Flock Safety to every restriction that applies to police. Vendors cannot retain copies of Arizona data beyond 30 days, cannot aggregate it with data from other states, cannot sell or share it, and cannot use it to develop commercial products. Flock operates in 5,000+ communities across 49 states.

Without this, every other restriction is cosmetic — the police department's local copy gets deleted while Flock retains a parallel national database.

> ***Amendment Language:***
>
> A. ALL PROVISIONS OF THIS ARTICLE THAT APPLY TO A LAW ENFORCEMENT AGENCY WITH RESPECT TO CAPTURED PLATE DATA SHALL APPLY WITH EQUAL FORCE TO ANY VENDOR THAT PROCESSES, TRANSMITS, STORES OR HAS ACCESS TO CAPTURED PLATE DATA.
>
> B. A VENDOR SHALL NOT:
>
> 1. RETAIN ANY COPY, BACKUP, DERIVATIVE OR REPRODUCTION OF CAPTURED PLATE DATA BEYOND THE AUTHORIZED RETENTION PERIODS.
> 2. AGGREGATE CAPTURED PLATE DATA WITH DATA COLLECTED IN ANY OTHER JURISDICTION OR FROM ANY OTHER SOURCE.
> 3. SHARE, SELL, LICENSE, PROVIDE ACCESS TO OR OTHERWISE MAKE AVAILABLE CAPTURED PLATE DATA TO ANY PERSON, ENTITY OR DATA-SHARING NETWORK OTHER THAN THE CONTRACTING ENTITY, EXCEPT PURSUANT TO A VALID WARRANT.
> 4. USE CAPTURED PLATE DATA FOR ANY COMMERCIAL PURPOSE, INCLUDING PRODUCT DEVELOPMENT, TRAINING OR IMPROVEMENT.
> 5. MAINTAIN A DATABASE OF CAPTURED PLATE DATA ACCESSIBLE TO PERSONS OTHER THAN THE CONTRACTING ENTITY.
>
> C. EVERY CONTRACT SHALL INCLUDE: compliance requirements, quarterly destruction certification, AG audit submission, and material breach/termination provisions.
>
> D. A VENDOR THAT VIOLATES THIS SECTION IS SUBJECT TO CRIMINAL PENALTIES (§28-1243(D)) AND CIVIL PENALTIES (§28-1255).

#3 Retroactive Query Controls with Supervisor Approval (§28-1244(B)(2), (C))

During the 30-day retention window, any retroactive search requires: (a) a documented felony case number, (b) written supervisor approval (sergeant+), and (c) full audit logging. Browsing without justification, non-felony queries, and "might be useful someday" fishing are explicitly prohibited. Storing data and freely browsing data are two fundamentally different things.

> ***Amendment Language:***
>
> B(2). A LAW ENFORCEMENT OFFICER MAY QUERY STORED CAPTURED PLATE DATA ONLY IF ALL OF THE FOLLOWING CONDITIONS ARE MET:
>
> (a) THE QUERY IS IN CONNECTION WITH A SPECIFIC, DOCUMENTED CRIMINAL CASE NUMBER FOR A FELONY OFFENSE.
>
> (b) A SUPERVISOR (SERGEANT+) HAS APPROVED THE QUERY IN WRITING, INCLUDING THE CASE NUMBER, PLATE/AREA TO BE QUERIED, TIME PERIOD, AND FACTUAL BASIS.
>
> (c) THE QUERY, SUPERVISOR'S APPROVAL AND RESULTS ARE RECORDED IN THE AUDIT LOG.
>
> C. THE FOLLOWING DO NOT CONSTITUTE LAWFUL ACCESS:
>
> 1. BROWSING WITHOUT A DOCUMENTED CASE NUMBER AND SUPERVISOR APPROVAL.
> 2. QUERYING FOR A NON-FELONY OFFENSE, GENERAL INCIDENT NUMBER, CITATION, CIVIL MATTER OR SPECULATIVE FUTURE USE.
> 3. QUERYING TO MONITOR ANY PERSON NOT A SUSPECT IN A DOCUMENTED FELONY INVESTIGATION.

#4 Exclusionary Rule (§28-1243(E))

Any ALPR data obtained in violation of this article — and any evidence derived from it — is inadmissible in any criminal, civil, or administrative proceeding. Without suppression, every other rule is a suggestion. The exclusionary rule is the only thing that makes the cost of cheating higher than the benefit.

Amendment Language:

E. CAPTURED PLATE DATA OBTAINED, RETAINED, ACCESSED OR SHARED IN VIOLATION OF THIS ARTICLE SHALL NOT BE ADMISSIBLE AS EVIDENCE IN ANY CRIMINAL, CIVIL OR ADMINISTRATIVE PROCEEDING IN THIS STATE. NO EVIDENCE DERIVED DIRECTLY OR INDIRECTLY FROM CAPTURED PLATE DATA OBTAINED IN VIOLATION OF THIS ARTICLE SHALL BE ADMISSIBLE. THIS SUBSECTION APPLIES REGARDLESS OF WHETHER THE VIOLATION WAS COMMITTED BY A LAW ENFORCEMENT OFFICER, A VENDOR OR ANY OTHER PERSON.

#5 30-Day Hard Retention Limit with Automatic Destruction (§28-1244(A))

All captured plate data is automatically and permanently destroyed after 30 days. Cannot be archived, backed up, or transferred to any system that would allow retention beyond 30 days without a warrant. The current bill has no maximum retention period — data can be kept forever.

Amendment Language:

A. CAPTURED PLATE DATA SHALL BE AUTOMATICALLY AND PERMANENTLY DESTROYED THIRTY DAYS AFTER THE DATE OF CAPTURE. DATA SHALL NOT BE RETAINED, ARCHIVED, BACKED UP OR TRANSFERRED TO ANY SYSTEM, SERVER OR STORAGE MEDIUM IN A MANNER THAT WOULD ALLOW RETENTION BEYOND THIRTY DAYS WITHOUT A WARRANT AS PRESCRIBED IN SUBSECTION D OF THIS SECTION.

TIER 2 — CLOSING THE BACKDOORS

These prevent the Tier 1 protections from being circumvented through workarounds, side channels, and legal loopholes.

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

Police need a warrant to access any private ALPR system — HOA cameras, business cameras, vendor databases. Standing agreements and MOUs are prohibited. Private entities that voluntarily share data without a warrant face $5K–$50K civil penalties. Flock’s model routes around government restrictions by selling to private entities who “voluntarily” share with police.

Amendment Language:

A. NO LAW ENFORCEMENT OFFICER SHALL ACCESS ANY PRIVATE ALPR SYSTEM WITHOUT FIRST OBTAINING A WARRANT BASED ON PROBABLE CAUSE.

B. DATA OBTAINED FROM A PRIVATE SYSTEM BY ANY MEANS SHALL BE SUBJECT TO ALL RESTRICTIONS OF THIS ARTICLE.

C. A PRIVATE ENTITY THAT VOLUNTARILY PROVIDES DATA WITHOUT A WARRANT: CIVIL PENALTY $5,000–$50,000 PER VIOLATION.

D. NO AGENCY SHALL ENTER INTO ANY AGREEMENT PROVIDING ACCESS TO A PRIVATE ALPR SYSTEM WITHOUT A WARRANT FOR EACH SPECIFIC QUERY.

#7 No Federal/Out-of-State Sharing Without an AZ Warrant (§28-1243(F)(3))

Arizona ALPR data cannot be shared with any federal agency (including ICE), any out-of-state agency, any private entity, or any vendor data-sharing network without a warrant from an Arizona court. Without this, Arizona data feeds a national surveillance grid regardless of local rules.

> ***Amendment Language:***
>
> 3. NOT SELL, SHARE, EXCHANGE OR PROVIDE CAPTURED PLATE DATA TO ANY FEDERAL AGENCY, INCLUDING UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT, ANY LAW ENFORCEMENT AGENCY OUTSIDE OF THIS STATE, ANY PRIVATE ENTITY OR ANY VENDOR-OPERATED DATA-SHARING NETWORK, EXCEPT PURSUANT TO A VALID WARRANT ISSUED BY A COURT OF COMPETENT JURISDICTION OF THIS STATE.
>
> IN-STATE SHARING: Only in connection with a specific documented criminal investigation, with date, time, reason and requesting agency documented in the system.

#8 Watchlist Governance (§28-1246)

Every watchlist entry requires a documented law enforcement basis and written supervisor approval. Entries auto-expire after 90 days. Bulk-loading for intelligence gathering or predictive policing is prohibited. The AG can audit the watchlist itself. If agencies can bulk-load thousands of plates, they bypass the retroactive query controls entirely.

> ***Amendment Language:***
>
> A. EACH ENTRY SHALL BE SUPPORTED BY A DOCUMENTED BASIS: CASE NUMBER, WARRANT NUMBER, NCIC ENTRY OR OFFICIAL RECORD.
>
> B. EACH ADDITION APPROVED IN WRITING BY SUPERVISOR (SERGEANT+), RECORDED IN AUDIT LOG WITH NAME, BADGE, DATE, CASE NUMBER AND REASON.
>
> C. ENTRIES AUTOMATICALLY EXPIRE AFTER 90 DAYS UNLESS RENEWED WITH WRITTEN CERTIFICATION.
>
> D. NO BULK-LOADING FOR GENERAL INTELLIGENCE, PREDICTIVE POLICING, OR VEHICLES NOT CONNECTED TO A SPECIFIC INVESTIGATION.
>
> E. ATTORNEY GENERAL HAS FULL AUDIT AUTHORITY OVER ANY ACTIVE WATCHLIST.
>
> F. ALL WATCHLIST ACTIVITY INCLUDED IN MONTHLY REPORTS.

#9 Closed “Official Purposes” List (§28-1241(2))

Changes “includes” to “means only the following” with an enumerated list. In Arizona statutory construction, “includes” means “includes but is not limited to.” This one-word change prevents scope creep at the definitional level.

> ***Amendment Language:***
>
> 2. “OFFICIAL LAW ENFORCEMENT PURPOSES” MEANS ONLY THE FOLLOWING:
>
> (a) IDENTIFICATION OF STOLEN OR WANTED VEHICLES AND STOLEN LICENSE PLATES.
>
> (b) IDENTIFICATION AND RECOVERY OF MISSING OR ENDANGERED PERSONS, INCLUDING AMBER AND SILVER ALERTS.
>
> (c) INVESTIGATION OF HUMAN TRAFFICKING.
>
> (d) GATHERING INFORMATION RELATED TO ACTIVE WARRANTS.
>
> (e) SUSPECT INTERDICTION AND STOLEN PROPERTY RECOVERY IN CONNECTION WITH A DOCUMENTED FELONY INVESTIGATION.
>
> (f) CANVASSING LICENSE PLATES IN THE IMMEDIATE VICINITY OF A DOCUMENTED CRIME SCENE.

#10 Warrant for Aggregation, Profiling, and Geofence Queries (§28-1245) ● ANTI-15-MIN CITY

Building movement histories, pattern-of-life analyses, and reverse location queries all require a warrant with specific particularity requirements. Zone-enforcement compliance monitoring is aggregation by definition, and no warrant could issue for a non-criminal travel-zone violation.

Amendment Language:

A. NO AGENCY SHALL ENGAGE IN AGGREGATION OR PROFILING WITHOUT A WARRANT BASED ON PROBABLE CAUSE.

B. WARRANT SHALL DESCRIBE: (1) the vehicle/person or location/time period, (2) the criminal investigation, (3) time period and geographic scope, (4) facts establishing probable cause.

C. NO WARRANTLESS BULK ANALYSIS, PATTERN-OF-LIFE ANALYSIS, HISTORICAL LOCATION TRACKING OR REVERSE LOCATION QUERIES.

D. REVERSE LOCATION QUERY = query to identify all vehicles at a specific location/area during a specific time period.

TIER 3 — ACCOUNTABILITY AND TRANSPARENCY

These ensure violations are detected, reported, and punished. They give the Tier 1 and 2 provisions real-world enforcement teeth.

#11 Felony Penalties with Tiered Structure (§28-1243(D))

Upgrades misuse from a $500 misdemeanor to Class 5–6 felonies. Permanent ban from ALPR access for anyone convicted.

Amendment Language:

D. CRIMINAL PENALTIES:

1. KNOWINGLY ACCESSES/USES/DISCLOSES FOR UNAUTHORIZED PURPOSE: CLASS 6 FELONY.
2. KNOWINGLY USES TO STALK, HARASS, INTIMIDATE OR TRACK: CLASS 5 FELONY.
3. KNOWINGLY SELLS OR PROVIDES TO UNAUTHORIZED ENTITY: CLASS 5 FELONY.
4. KNOWINGLY CIRCUMVENTS AUTO-DESTRUCTION MECHANISMS: CLASS 6 FELONY.
5. RECKLESSLY ACCESSES/USES/DISCLOSES/FAILS TO DESTROY: CLASS 1 MISDEMEANOR.
6. CONVICTED PERSON PERMANENTLY PROHIBITED FROM ACCESSING ANY ALPR SYSTEM IN THIS STATE.

#12 Private Right of Action with Immunity Waiver (§28-1255)

Citizens can sue for actual damages, $2,500+ statutory damages per violation, attorney fees, and injunctive relief. Sovereign and qualified immunity explicitly waived. Each unauthorized access counts as a separate violation.

Amendment Language:

A. CIVIL ACTION IN SUPERIOR COURT FOR: (1) actual damages, (2) statutory damages ≥$2,500 per violation, (3) attorney fees and costs, (4) injunctive relief including data destruction orders.

B. EACH INSTANCE OF UNAUTHORIZED COLLECTION, RETENTION, ACCESS, SHARING OR USE IS A SEPARATE VIOLATION.

C. SOVEREIGN IMMUNITY AND QUALIFIED IMMUNITY SHALL NOT BE A DEFENSE.

#13 Mandatory Monthly AG Reporting with Auto-Suspension (§28-1253(A)–(B))

Monthly reports to the AG covering all system activity. Miss the 30-day deadline = all ALPR operations automatically shut down until filed and accepted.

> ***Amendment Language:***
>
> A. MONTHLY REPORT TO AG INCLUDING: devices/locations, plates scanned, matches, retroactive queries (with case numbers), watchlist changes, warrants obtained, citizen requests, deletion requests, unauthorized access/misuse instances.
>
> B. FAILURE TO SUBMIT WITHIN 30 DAYS = IMMEDIATE MANDATORY SUSPENSION OF ALL ALPR OPERATIONS UNTIL REPORT IS FILED WITH AND ACCEPTED BY THE ATTORNEY GENERAL.

#14 Mandatory Annual AG Audits (§28-1253(D)–(E))

The AG "shall conduct at least one audit per year of each agency" — mandatory, not optional. Scope includes devices, servers, vendor systems, watchlist entries, and all authorization records. The original bill used "may."

> ***Amendment Language:***
>
> D. THE ATTORNEY GENERAL SHALL CONDUCT AT LEAST ONE AUDIT PER YEAR OF EACH AGENCY. SCOPE: ALPR devices, all servers, all vendor systems/records, watchlist entries, retroactive query approvals, supervisor authorization records.
>
> E. THE ATTORNEY GENERAL MAY SEEK INJUNCTIVE RELIEF INCLUDING AN ORDER PROHIBITING ALPR USE BY ANY AGENCY OR VENDOR FOUND IN VIOLATION.

#15 Transparency Portal with Camera Locations (§28-1252(A))

Public online portal showing: location of every fixed camera, plates scanned, matches, retroactive queries, stops/arrests, system errors, and every entity data was shared with — including date, purpose, and legal authority.

> ***Amendment Language:***
>
> A. PUBLICLY ACCESSIBLE ONLINE TRANSPARENCY PORTAL DISPLAYING:
>
> 1. LOCATION OF EACH FIXED ALPR DEVICE (BY INTERSECTION/ADDRESS).
> 2. TOTAL LICENSE PLATES SCANNED IN PRECEDING MONTH.
> 3. POSITIVE MATCHES GENERATED.
> 4. RETROACTIVE INVESTIGATIVE QUERIES CONDUCTED.
> 5. VEHICLE STOPS, SEARCHES, ARRESTS FROM ALPR ALERTS.
> 6. SYSTEM ERRORS, FALSE POSITIVES, DATA BREACHES.
> 7. IDENTITY OF EVERY ENTITY DATA WAS SHARED WITH, INCLUDING DATE, PURPOSE AND LEGAL AUTHORITY.

TIER 4 — CITIZEN RIGHTS AND HOA/SCHOOL PROTECTIONS

These protect individual rights and extend the regulatory framework beyond law enforcement to the private ALPR systems most likely to be scanning your plate daily.

#16 HOA ALPR Requirements (§28-1249)

Requires majority homeowner vote before deploying cameras. 30-day retention. No sharing with police without a warrant. Security-only use. Signage. Written data policy. Resident data access and deletion. $5K–$50K civil penalties. AG enforcement.

Amendment Language:

A. REQUIREMENTS: (1) majority recorded vote, (2) 30-day retention with auto-destruction, (3) no sharing with law enforcement without warrant, (4) security-only use, (5) signage at all entrances, (6) written data policy, (7) resident data access and deletion within 10 business days.

B. VENDOR CONTRACTS: must prohibit warrantless sharing, aggregation, retention past 30 days, and grant audit rights.

C. CIVIL PENALTY: $5,000–$50,000 PER VIOLATION. EACH DAY IS A SEPARATE OFFENSE.

D. ATTORNEY GENERAL MAY INVESTIGATE AND BRING CIVIL ACTION.

#17 School District ALPR Requirements (§28-1250)

Public board vote with 30 days' notice. Campus security use only. Cameras cannot photograph occupants including students. 30-day retention, warrant-only sharing. Cannot monitor/track/discipline students. Plate data = FERPA student records.

Amendment Language:

A. REQUIREMENTS: (1) board vote at public meeting with 30 days' notice to parents, (2) campus security use only, (3) cameras cannot photograph vehicle occupants, (4) 30-day retention, (5) no sharing without warrant, (6) cannot monitor/track/discipline students or families, (7) signage, (8) written public policy.

C. CAPTURED PLATE DATA IS A STUDENT RECORD UNDER FERPA (20 USC §1232g) TO THE EXTENT IT IDENTIFIES A STUDENT OR FAMILY.

D. CIVIL PENALTY: $5,000–$50,000 PER VIOLATION.

E. ATTORNEY GENERAL MAY INVESTIGATE AND BRING CIVIL ACTION.

#18 Citizen FOIA Access to Own Data (§28-1254)

Right to obtain all ALPR data about your own vehicle — images, capture dates/times/locations, access log, and sharing history. Free first request per year. Cannot be denied on exemption grounds.

Amendment Language:

A. RIGHT TO OBTAIN: (1) all images of your vehicle, (2) dates/times/locations of captures, (3) log of every person/agency that accessed your data, (4) whether data was shared and identity of recipients.

B. RESPONSE WITHIN 15 BUSINESS DAYS. NO FEE FOR FIRST REQUEST PER 12 MONTHS.

C. AGENCY SHALL NOT DENY REQUEST ON EXEMPTION GROUNDS.

#19 Citizen Data Deletion Requests (§28-1252(C)–(D))

Right to request deletion if data is not part of an active investigation. Agency must comply within 10 business days. 1-year cap on the investigation exemption.

Amendment Language:

C. A RESIDENT MAY REQUEST DELETION OF DATA NOT ASSOCIATED WITH AN ACTIVE INVESTIGATION. AGENCY SHALL COMPLY WITHIN 10 BUSINESS DAYS AND CONFIRM IN WRITING.

D. INVESTIGATION EXEMPTION LIMITED TO ONE YEAR. AFTER ONE YEAR, AGENCY SHALL PROVIDE ALL RESPONSIVE DATA (REDACTED AS NECESSARY) WITHIN 30 DAYS.

#20 Mandatory Verification Before Stops (§28-1242(C))

A positive match alone is not reasonable suspicion. Officers must visually verify the plate and confirm through dispatch/NCIC that it remains on an active watchlist before making a stop.

Amendment Language:

C. A POSITIVE MATCH ALONE SHALL NOT CONSTITUTE REASONABLE SUSPICION. BEFORE TAKING ENFORCEMENT ACTION, AN OFFICER SHALL:

1. VISUALLY VERIFY THE LICENSE PLATE MATCHES THE ALPR IMAGE.
2. CONFIRM THROUGH DISPATCH, NCIC OR OTHER INDEPENDENT MEANS THAT THE PLATE REMAINS ON AN ACTIVE WATCHLIST.

TIER 5 — STRUCTURAL SAFEGUARDS

These prevent long-term mission creep and protect local democratic authority over surveillance decisions.

#21 Local Control with Anti-Circumvention (§28-1251) ● ANTI-15-MIN CITY

Communities can ban ALPRs by ordinance. If they do, no outside agency — including the county sheriff, MCSO, DPS, or any state agency — can deploy cameras within that community. Interstate highway exception only, capped at pre-ban levels. The Oxford model was imposed top-down over voter objections. This ensures that cannot happen in Arizona.

Amendment Language:

A. A CITY, TOWN OR COUNTY MAY PROHIBIT ALPR DEPLOYMENT OR OPERATION WITHIN ITS BOUNDARIES.

B. IF A LOCAL GOVERNMENT PROHIBITS ALPRs, NO OTHER AGENCY (INCLUDING COUNTY SHERIFF, MCSO, DPS OR ANY STATE AGENCY) SHALL DEPLOY, OPERATE OR MAINTAIN ALPRs WITHIN THOSE BOUNDARIES.

C. EXCEPTION: Mobile readers on interstate highways only, for official purposes only, capped at pre-ban deployment levels, not deployed on any non-interstate road.

#22 Three-Year Sunset Clause (§28-1256) ● ANTI-15-MIN CITY

Entire article repealed January 1, 2029 unless the Legislature affirmatively reauthorizes. Forces recurring public debate as the technology evolves. Insurance policy against uses that do not exist yet.

Amendment Language:

28-1256. REPEAL

THIS ARTICLE IS REPEALED FROM AND AFTER JANUARY 1, 2029.

#23 Camera Capability Restrictions (§28-1242(G))

ALPR cameras must read plates only. Cannot photograph, record, or produce images of vehicle occupants. Prevents function creep into general video surveillance and facial recognition.

Amendment Language:

G. AN AUTOMATED LICENSE PLATE READER SHALL BE INSTALLED AND CONFIGURED FOR THE SOLE PURPOSE OF READING AND CHECKING LICENSE PLATES. AN AUTOMATED LICENSE PLATE READER SHALL NOT BE CAPABLE OF PHOTOGRAPHING, RECORDING OR PRODUCING IMAGES OF THE OCCUPANTS OF A MOTOR VEHICLE.

#24 Warrant Cap for Extended Retention (§28-1244(D)–(E))

Warrant renewals limited to 3 times. Each renewal requires showing evidence was produced or expected. Absolute maximum: 1 year from capture. Prevents indefinite retention through rubber-stamped warrant chains.

Amendment Language:

D. WARRANT REQUIRED FOR RETENTION BEYOND 30 DAYS. SHALL SPECIFY: (1) specific plates/vehicles, (2) criminal investigation, (3) probable cause facts, (4) additional period not exceeding 90 days.

E. WARRANT MAY BE RENEWED NOT MORE THAN 3 TIMES. DATA SHALL NOT BE RETAINED FOR MORE THAN ONE YEAR FROM ORIGINAL CAPTURE REGARDLESS OF WARRANTS.

#25 Remove Blanket Public Records Exemption (§28-1243(B))

The original bill exempts 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.

Amendment Language:

B. THE FOLLOWING ARE PUBLIC RECORDS SUBJECT TO TITLE 39, CHAPTER 1, ARTICLE 2:

1. ALL AGENCY POLICIES AND PROCEDURES GOVERNING ALPR USE.
2. AUDIT LOGS (WHO ACCESSED, WHEN, AND WHY).
3. AGGREGATE STATISTICAL REPORTS ON SYSTEM USAGE.
4. RECORDS OF DISCIPLINARY ACTIONS FOR UNAUTHORIZED USE.
5. MONTHLY AND ANNUAL REPORTS REQUIRED PURSUANT TO §28-1253.