

AUBURN CITY COUNCIL STAFF REPORT

TO:	Honorable Mayor and Members of the City Council
FROM:	Bryan Morrison, Chief of Police
BUSINESS TYPE:	Council Business
MEETING DATE:	October 12, 2026
SUBJECT:	Report Back on the City's use of the Automatic License Plate Reader system

Action Requested

Staff requests that the City Council receive the report and provide direction on creating a City policy to guide the use of the Automated License Plate Reader system.

Strategic Plan Alignment:

The requested action supports the City's Strategic Plan priorities of Organizational Trust, Quality of Life and Community Wellbeing, and Community Engagement and Transparency by providing the City Council with information necessary to evaluate the continued use of the Automated License Plate Reader system.

Background

The City of Auburn Police Department (APD) utilizes an Automated License Plate Reader (ALPR) system provided by Flock Safety. ALPR technology uses cameras to capture images of vehicles and license plates and can assist law enforcement personnel in identifying vehicles associated with criminal investigations. The system is an investigative tool and is intended to supplement, rather than replace, traditional law enforcement investigative practices.

APD currently utilizes Flock ALPR cameras at locations throughout the City of Auburn. The system provides authorized personnel with investigative capabilities assistance in developing leads, identifying vehicles associated with criminal activity, and supporting active investigations. The Department has established policies, training requirements, and oversight measures governing the use of the system.

Beginning with the August 10, 2026, City Council meeting, members of the community began expressing concerns regarding the City of Auburn's use of the Flock ALPR system during the Public Comment portion of City Council meetings.

At the subsequent City Council meeting on August 24, 2026, additional members of the community spoke during Public Comment regarding the Auburn Police Department's use of the Flock ALPR system. The majority of those who spoke expressed opposition

to the City's continued use of the system; however, two community members spoke in support of the Flock ALPR system.

At the September 14, 2026, City Council meeting, Mayor Davis announced that the City of Auburn would host a Town Hall meeting to be held on September 21, 2026, and would provide the community with an opportunity to learn more about how the Auburn Police Department uses the Flock ALPR system and to ask questions of City staff.

On September 21, 2026, the City of Auburn hosted a Town Hall meeting in the Rose Room at City Hall. The meeting provided an opportunity for City staff to present information about the Flock ALPR system and for members of the community to ask questions and express how they feel about the system.

During the Town Hall, staff provided an overview presentation regarding how the Flock ALPR system is utilized by the Auburn Police Department. The presentation included information regarding the City's contract with Flock, the number and general deployment of ALPR cameras throughout the City, the purpose for which the system is used, how authorized personnel use the system, and the capabilities and limitations of the technology. The presentation also addressed Fourth Amendment considerations associated with the use of ALPR technology, provided real-world case examples in which Flock ALPR technology assisted the Department with active investigations, and included information regarding the live camera feeds deployed by the City of Auburn.

Following the presentation, City staff opened the floor for public questions and comments. Staff were able to answer many of the questions presented during the Town Hall. Several questions, however, required additional research, clarification, or information that was not immediately available to staff. Following the Town Hall, staff conducted additional research and sought clarification regarding the outstanding questions and additional questions received after the Town Hall. The questions and answers are summarized in Attachment B.

The purpose of this staff report is to provide the City Council with a consolidated record of the information presented at the Town Hall and the additional information subsequently obtained by staff. This information is intended to assist the City Council in evaluating the use of the Flock ALPR system and in providing direction regarding creating a City policy adopted by the City Council to provide parameters on the use of the system in the City of Auburn.

Adoption of a City ALPR policy allows an opportunity for public input, establish clear governance and privacy standards for ALPR use, and promote transparency and public trust. Elements of a policy could include the following:

- Authorized and Prohibited Uses

- Data Collection, Access, Storage, Retention, and Protection
- Third-Party Data Sharing
- Training
- Oversight

Enhancing these measures would allow the Department to better address the concerns raised by members of the community while maintaining an investigative resource that can assist officers in developing leads and identifying vehicles associated with crimes that may directly impact members of the community.

Staff believe these additional safeguards can provide greater accountability and transparency while preserving the Department's ability to utilize ALPR technology as an investigative tool in support of public safety.

Alternatives to Recommended Action

1. Direct staff to immediately terminate the contract with Flock Safety ending the use of their ALPR cameras within the City.
2. Direct staff to continue utilizing the Flock ALPR system with no additional City Council policy development.

CEQA Requirements

This action does not impact CEQA requirements.

Fiscal Impact

The City's current agreement with Flock provides for an annual cost of approximately \$30,000 per year for the City's existing ALPR system. If the City continues the agreement through the end of the current June 2028 contract term, the City will continue to incur this annual expenditure through the expiration of the agreement.

If the City elects to terminate the agreement prior to the expiration of the contract term, the City would be subject to the applicable early termination provisions contained within the agreement. The contract currently provides that termination for convenience will result in a one-time fee of \$500 per Flock Hardware unit. Based on the City's current deployment of 12 Falcon cameras, the anticipated termination cost would be a minimum \$6,000, subject to confirmation from Flock regarding the contractual definition and calculation of "Flock Hardware."

Attachments

- A. Town Hall presentation
- B. Answers to questions from the Town Hall meeting that went unanswered and questions received after the Town Hall
- C. Sample ALPR policies from other CA cities

- D. CA Police Chief's Association policy framework
- E. American Civil Liberties Union model privacy bill

Automated License Plate Reader (ALPR) Overview

MEETING AGENDA

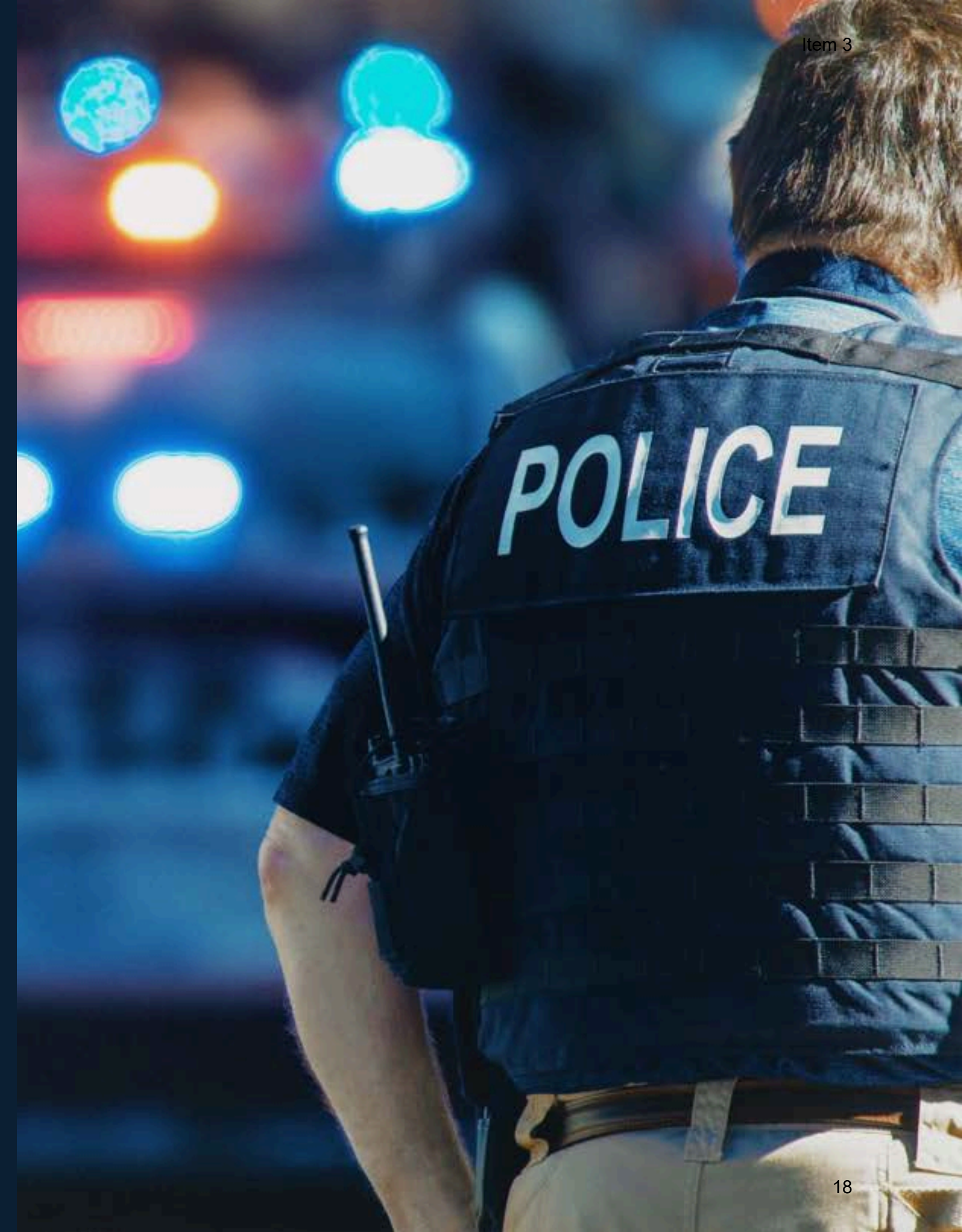
1. Welcome and Introduction
2. Presentation
3. Questions and Comments

Next Meeting Date:
Tentatively Scheduled for October 12, 2026

Auburn Police Department
SEPTEMBER 21, 2026

WHY AUBURN USES ALPR

- Staffing levels limit the PD's presence
- ALPR serves as a force multiplier
- Can complement and enhance the deterrent effect of police presence
- Provides investigators with rapid investigative leads
- Allows officers to work more efficiently with existing resources
- Cost-effective - Reduces costs associated with hours worked
- Expedited 230 case investigations
 - (29) stolen vehicles, (14) Burglary, (11) hit-and-run, (11) missing persons, (27) violent crimes



Personnel Deployment Structure

PATROL TEAMS

2 Officers + 1 Sergeant

12-hour shifts • one team active per shift

INVESTIGATIONS

3 internal + 1 task force

SCHOOL
RESOURCE

1 Officer

This depicts the staffing levels APD is currently budget for and does not account for training, vacation, or sick leave vacancies.

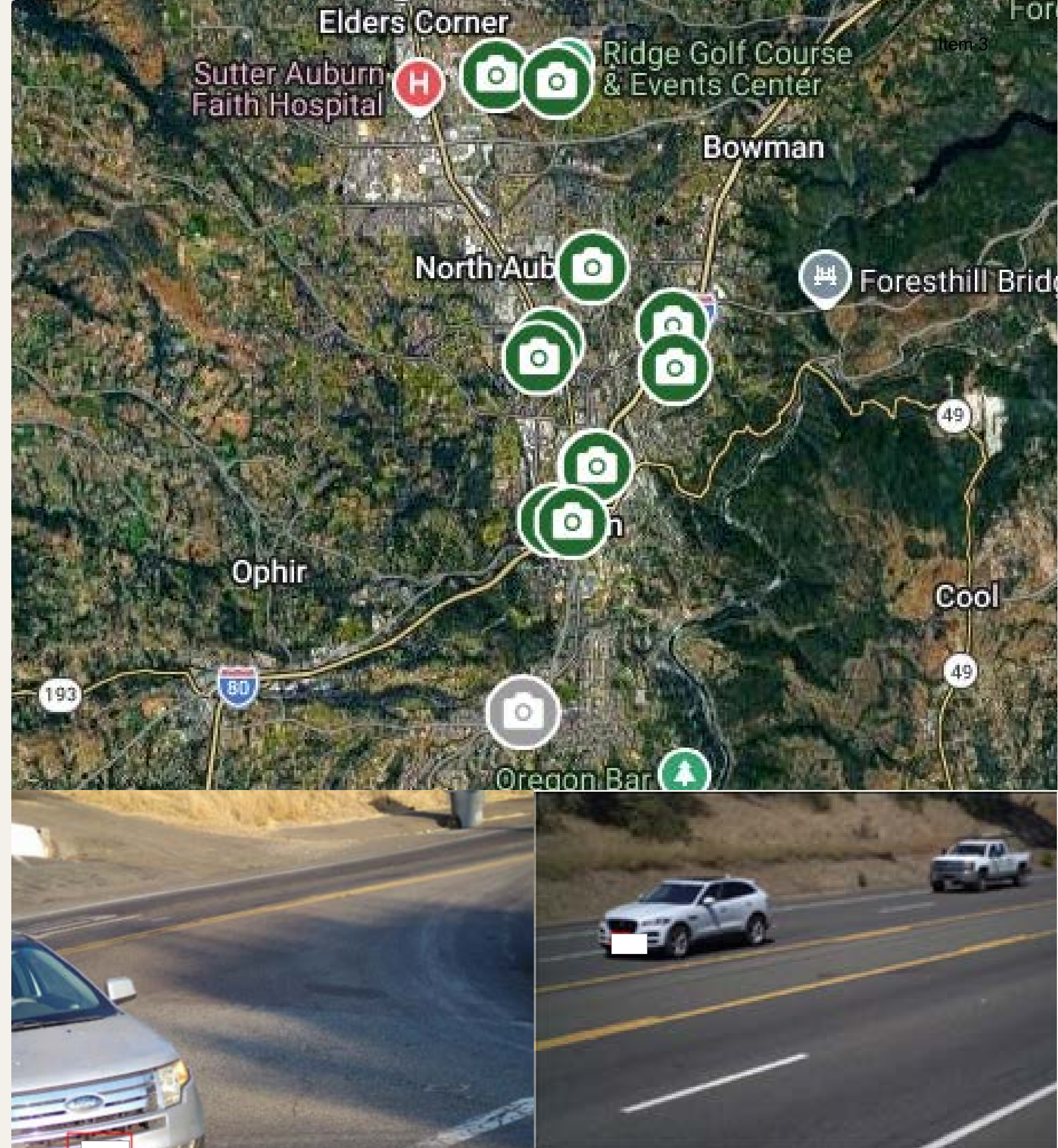
ALPR System Overview

12 ALPR Cameras

First camera installed August 2022

Contract through June 2028

- Captures license plates and vehicle characteristics
- Positioned to capture rear license plates and vehicle information while minimizing unnecessary collection of occupant information
- Cameras are not positioned at inner-city intersections to "track" individual movements



How Auburn PD Uses ALPR

- Primarily an investigative tool
- Searches may use:
 - Full license plates
 - Partial plates
 - Vehicle descriptions
 - Vehicles associated with investigations or wanted persons
- Officers follow up on verified ALPR alerts that can be linked to a stolen vehicle, wanted person, missing person, etc.
- Staff does not conduct random searches of specific license plates without a legitimate law-enforcement purposeS
- Increase Officer and community safety

No random or unjustified searches. The objective is community and officer safety.

Data and Sharing

- 30-day data retention - set at 30 days to account for delayed reporting
- Out-of-state and federal agency sharing disabled
- Searches require offense type
- Allows integration into the network operating system - a tool to help locate vehicles associated with being stolen, subjects implicated in crimes, and missing loved ones who have left Auburn or come to Auburn from another jurisdiction
- Types of sharing
 - Mutual Sharing
 - One way sharing

Search Type: All types Start Date & Time: 08/22/2026 12:00 AM End Date & Time: 09/21/2026 09:21 AM Update

☒ Include all records of searches on my networks ☐ Include only out-of-state searches

Network Audit Results [Download CSV](#)

ID	Name	Org Name	Networks	Time Frame	License Plate	Reason	Case #	Filters	Search Time	Search Type
abed9dea-e585-4299-9b3f-17377d310d0d	***	San Jose CA PD	538 Networks	September 20, 2026 9:30 AM September 21, 2026 9:30 AM	***	Assault/Battery Offenses	***		September 21, 2026 9:21 AM	Lookup
533ac99b-3630-47f9-908b-961484839dd3	***	Tulare County CA SO	198 Networks	August 22, 2026 9:30 AM September 21, 2026 9:30 AM	***	Alcohol Offenses (Non-DUI) - Investigation			September 21, 2026 9:21 AM	Lookup
aa1804f9-0c55-49c4-82ff-b4513b3818d0	***	Riverside County CA SO	840 Networks	September 20, 2026 9:30 AM September 21, 2026 9:30 AM	***	Larceny/Theft Offenses - 488	***		September 21, 2026 9:21 AM	Lookup
0bd738de-c302-444c-af57-21725d0d049d	***	Riverside County CA SO	840 Networks	September 7, 2026 9:30 AM September 21, 2026 9:30 AM	***	Human Trafficking - HT INV Missing Juvs	***	***	September 21, 2026 9:20 AM	Lookup
8e28b358-0875-4f3f-a049-369e133568ad	***	Riverside County CA SO	772 Networks	September 20, 2026 9:20 AM September 21, 2026 9:20 AM	***	Wanted Person (Arrest Warrant/Fugitive) - Investigation	***		September 21, 2026 9:20 AM	Lookup - Mobile
237d76fb-fdbf-4513-a5bf-6cf31c30f114	***	Riverside County CA SO	926 Networks	August 22, 2026 9:30 AM September 21, 2026 9:30 AM	***	Burglary/Breaking & Entering - 459 sus veh	***	***	September 21, 2026 9:20 AM	Lookup
598738a2-6c0e-4336-a1e5-80017c0560db	***	Sunnyvale CA PD	697 Networks	September 20, 2026 9:30 AM September 21, 2026 9:30 AM	***	Assault/Battery Offenses (Domestic)			September 21, 2026 9:20 AM	Lookup

Network Audit

NOTE: Search Reason and Case Number field inputs will depend on each individual organization's requirements. If the record contains ***, it means that information exists, but is only visible to the searching agency. Reach out to the searching agency to discuss additional details if needed.

Filters

Search Type: All types Start Date & Time: 08/22/2026 12:00 AM End Date & Time: 09/21/2026 09:21 AM Update

☒ Include all records of searches on my networks ☒ Include only out-of-state searches

No data found for report

ALPR Checks and Balances Workflow

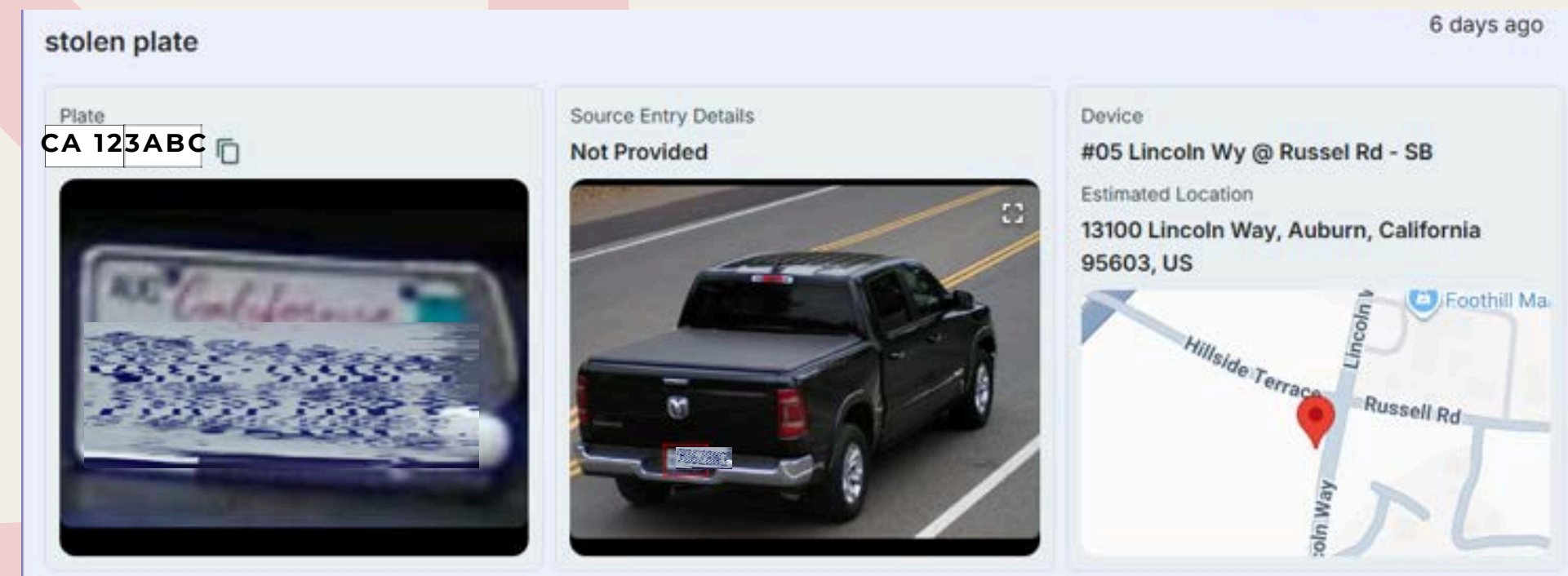


- Dispatch compares the alert against the actual plate
- Dispatch determines whether the alert is a match
- Dispatch checks National Crime Information Center and/or jurisdiction responsible for entry to confirm the vehicle remains wanted
- Officers verify the plate before initiating enforcement
- If an officer encounters the vehicle before dispatch completes verification, the officer confirms the plate while dispatch completes the verification process
- These safeguards help minimize false alerts and erroneous enforcement actions
- To date, APD has not conducted any felony stops related to and ALPR misread

All alert types do not mandate a specific police tactic or response. Patrol staff are encouraged to use discretion to determine their response to an alert based on the totality of the circumstances.

What Auburn Police ALPRs Do Not Do

- **FACIAL RECOGNITION**
- **IDENTIFY BY GENDER OR RACE**
- **BIOMETRIC STORAGE**
- **QUERIES TO FIND PEOPLE**
- **LIVE PTZ OR TRACKING**
- **ICE ARRESTS / INVESTIGATIONS**
(WOULD NOT AND CAN NOT LEGALLY)
- **DIRECT DMV INTERFACE**
(Requires a separate, need-to-know / right-to-know lookup)



Accountability and Privacy Protections

- ✓ Defined law-enforcement purpose
- ✓ External sharing restrictions
- ✓ Justification requirements
- ✓ Search auditing
- ✓ Verification before enforcement action
- ✓ Vendor accountability
- ✓ Limited retention – 30 days
- ✓ Policy-driven use



Auburn CA PD Transparency Portal

Last updated: Mon Sep 14 2026

Community Impact

Data & Usage Summary

Data Retention
The number of days data is retained.

30 days

Total Cameras
Number of LPR and other cameras.

12

Vehicles detected in the last 30 days Number of unique plate reads over the last 30 days.	Number of Searches Total user search requests over the last 30 days.
178,268	95

Hotlines Alerted On National and statewide hotline sources.	Number of Hotlist Hits Total hotlist hits over the last 30 days.
California EVIS, NCMEC Amber Alert	312

Sharing Network Data With

Organizations granted access to Auburn CA PD data.

- Alameda County CA SO
- Amador County CA Sheriff's Office
- Anderson CA PD
- Antioch CA PD
- Atwater CA PD
- Azusa CA PD

Policy & Trust

What's Detected

License Plates, Vehicles

What's Not Detected

Facial recognition, People, Gender, Race

Acceptable Use Policy

Data is used for law enforcement purposes only. Data is owned by Auburn CA PD and is never sold to 3rd parties.

Prohibited Uses

immigration enforcement, traffic enforcement, harassment or intimidation, usage based solely on a protected class (i.e. race, sex, religion), Personal use.

Access Policy

All system access requires a valid reason and is stored indefinitely.

Hotlist Policy

Hotlist hits are required to be human verified prior to action.



<https://transparency.flocksafety.com/auburn-ca-pd>

SCAN THE QR CODE OR VISIT THE LINK ABOVE TO VIEW
OUR FLOCK TRANSPARENCY PORTAL.

INTERESTED IN AN OFFICER RIDEALONG OR DISAPTCH SIT-ALONG?

Get a behind-the-scenes look at how the Auburn Police Department
serves our community! Scan the QR Code to Apply.



Fourth Amendment Legal Context

2018

Carpenter v. United States

United States Court case that continues to be highlighted is Carpenter vs. United States

- This case was related to cell-site location information where officials obtained over 12,898 location data points over 127 days allowing reconstruction of Carpenter's movements to include private locations
- In a narrow 5-4 ruling the court ruled a search warrant based on probable cause is required to obtain data.

2026

Schmidt v. City of Norfolk

- The city's cameras only implicated movements in public streets, not private locations.
- The court also noted that the city's 176 cameras were installed in about 75 distinct locations did not cover the entire city.
- The court contrasted the city's ALPR cameras with Carpenter, where the cell phone data followed the defendant to private locations
- In contrast, the city's ALPR cameras only capture that a vehicle was at the location of the camera and the camera network was not so constant as to capture every movement of a person or a vehicle.
- Further, there were often pronounced gaps between multiple data points on the same day, which demonstrated the current limits of the technology.
- Court ruled the city's ALPR cameras did not violate a reasonable expectation of privacy.

No U.S. Supreme Court decision has held ALPR unconstitutional. Courts assess the specifics of each system.

ALPR: Real-World Public Safety Results

Auburn Police Department - Parental Child Abduction

- ALPR-generated information assisted in locating a suspect in an adjoining county
- Child was safely reunited with the custodial parent
- Benefits of being a part of the operating system

Auburn Police Department - Internet Crimes Against Children Investigation

- Following up on an Internet Crimes Against Children lead, detectives identified a person of interest and authored a search warrant, which was subsequently signed by a judge.
- The warrant was served at an Auburn residence, where significant evidence was recovered.
- The suspect was out of town when the warrant was served and, after being alerted by family members, quick his local job and fled.
- Investigators entered the suspect vehicle into the ALPR system, which ultimately led to the suspect's arrest in Southern California.

Benefits of being apart of the operating system: Arrest and likely prevented others falling victim to the suspect in this case

ALPR: Real-World Public Safety Results

Colfax - Armed Robbery

Though not in our jurisdiction, but a recent example within Placer County where an ALPR system was used as an investigative tool in developing a lead to take a armed and potentially dangerous suspect off the street who resided in a neighboring county.

Sacramento County Homicide (September 2026)

- 36-year-old female was shot and killed near a local business on Howe Ave.
- The suspect who was identified as stalking the victim fled the scene in a vehicle after committing the homicide
- Within 7 minutes of committing the homicide, through an investigative lead utilizing an ALPR system, the suspect vehicle was located on Highway 50 near Watt Ave
- The suspect barricaded himself in his vehicle and later determined to have suffered a self inflicted gun shot wound

ALPR: Real-World Public Safety Results

Sacramento Police Double Homicide (September 2017)

- Prior week two woman were murdered in a south Sacramento residence
- Investigators were able to develop leads ultimately Identifying a suspect
- The suspect's vehicle was entered into ALPR system
- ALPR captured and alerted Sacramento PD officers that the suspect vehicle was mobile
- Patrol located the vehicle and followed it until enough units safely conduct a vehicle stop
- The suspect initially cooperated and within seconds quickly jumped out of the vehicle and began shooting at the officers
- Ultimately two officers sustained moderate to significant injuries and the suspect succumbed to injuries sustained in the gun battle.

Several Hit and Runs

Multiple Missing/ At Risk Persons Cases

Live-Feed Cameras, Auburn City Limits

- Police Department
- Airport
- City Hall
- Chamber of Commerce
- City Parks

Provide live camera feeds – pan, tilt, zoom

Have self-moving / tracking software



Uses of Live-Feed Cameras

Monitor locations and dispatch patrol officers as a preventative measure when incidents begin to unfold.

PREVENT

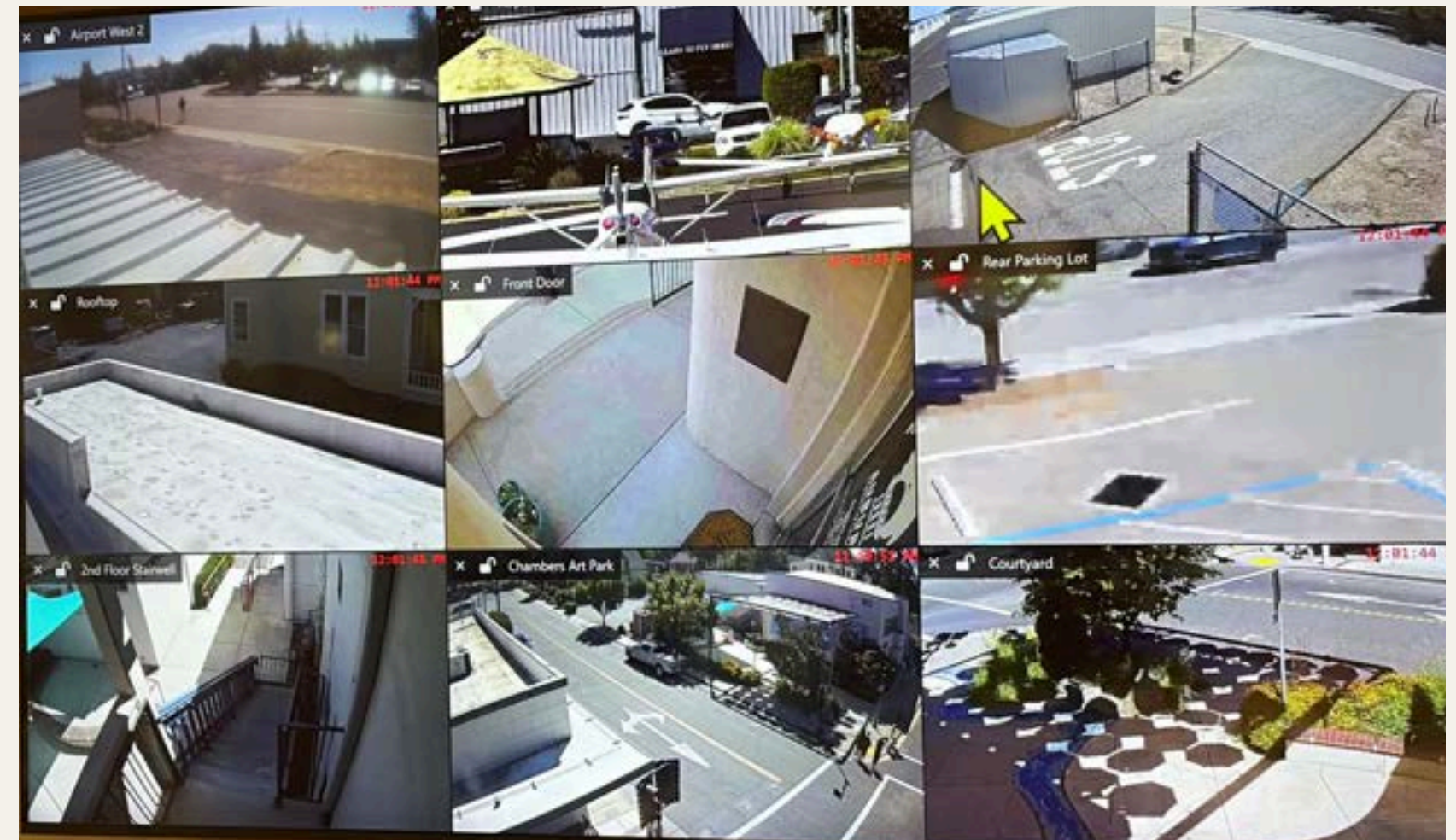
Early response dispatch and visible deterrence

UNDERSTAND

Develop investigative leads and monitor evolving scenes

PROTECT

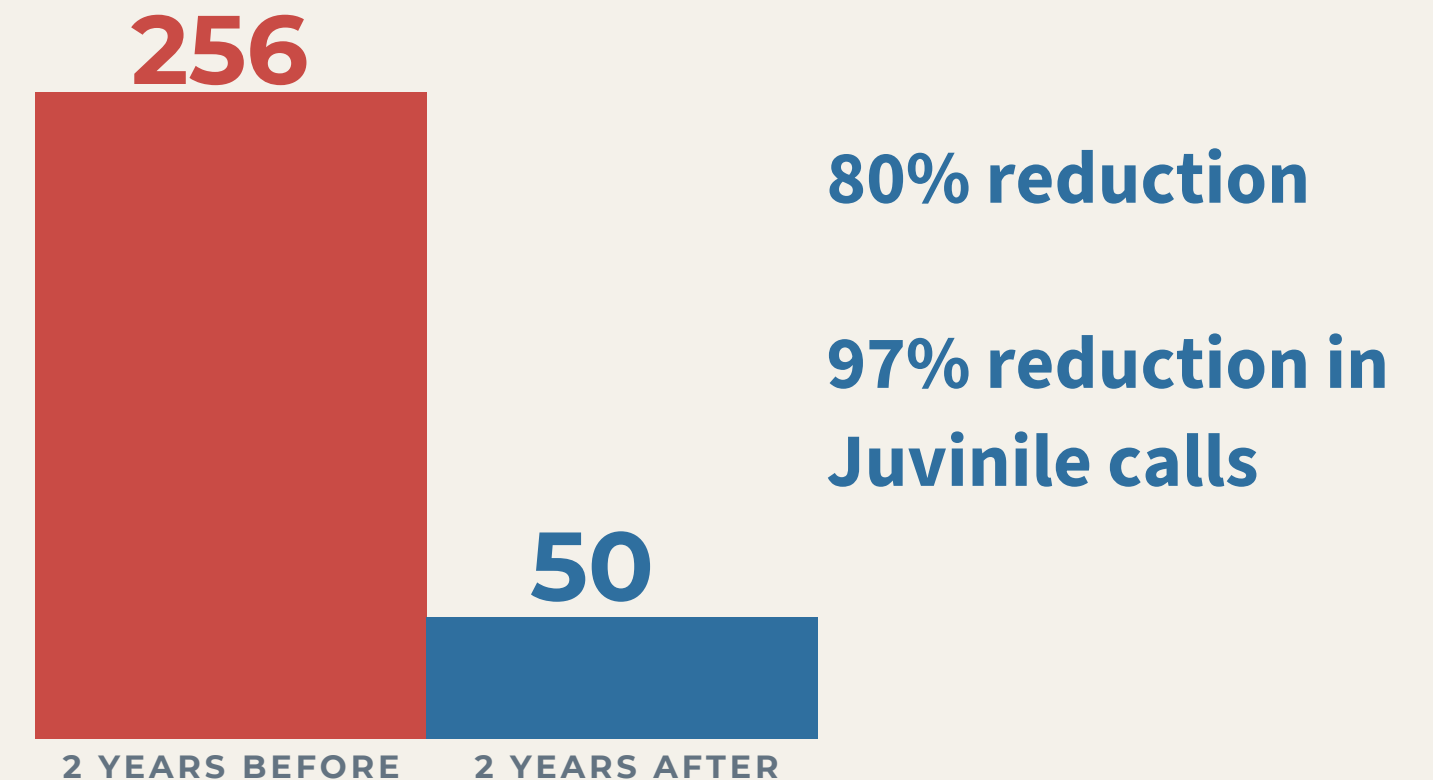
Improve officer and community safety



Real Life Success Stories from Live-Feed Cameras

School Park Preserve

- Installed May 29, 2023 after PD resources (dispatch, patrol officers, school resource officer, and detectives) were being inundated with calls for service within the park.
- Before the cameras were installed, a two year span revealed PD staff was involved in 256 calls for service. A two year span after the cameras were deployed revealed PD staff was involved in only 50 calls for service (80% reduction). We experienced a 97% reduction in calls entered a “juvenile problem” during same respective two year span before and after the camera were installed



Threat of Active Shooter at the Airport

- Received the call which generated an immediate police response
- Allowed for dispatch to monitor the airport to provide live updates
- Ultimately building grounds to believe this was a hoax
- Promoted a safer (officer/community) response as we were able to weigh the degree of exigency
- Provide live updates and potential threat locations while staff was actively clearing the grounds



TECHNOLOGY + PEOPLE + ACCOUNTABILITY

Together, keeping Auburn safe.



ALPR extends the effectiveness of a small department. Technology supports officers and community safety — with verification, policy and accountability built in.



ALPR Questions and Answers

October 8, 2026

1. What agencies have access to our data captured by our ALPR system and what agencies have granted us access to their data captured by their ALPR system?

Auburn Police Department

ALPR Network Sharing Summary

Source: Flock Shared Networks export, current as of October 1, 2026.

At a Glance	Agencies
Agencies Auburn PD shares data with	274
Agencies sharing data with Auburn PD	197
Agencies sharing both ways	180
Auburn shares with them only	94
They share with Auburn only	17
Camera networks shared with Auburn PD	511
Out-of-state or federal agencies	0

2. Provide all the intersections where ALPR cameras are located.

Lincoln Wy @ Russel Rd
 Auburn Ravine Rd @ Nation Dr
 Dairy Rd @ Luther Rd
 Nevada St @ Placer St
 Marguerite Mine Rd @ Nevada St
 Marguerite Mine Rd @ Nevada St
 Auburn Folsom Rd @ Indian Hill Rd
 Elm @ SB 80 Offramp
 Maple St @ Union St
 Nevada St @ S/O Nevada Wy
 New Airport Rd @ Old Airport Rd

Earhart Ave @ Wilbur Way
Auburn Town Center @ Elm Ave Entrance

3. How many people at the PD have access to our Flock system?

21 Full Time Officers
8 Professional Staff
4 Reserve Police Officers

4. How many people at the PD are administrators having the ability to authorize sharing?

Police Chief, two Lieutenants, Administrative Sergeant, and Communications Supervisor

5. Please provide big picture training on what training is provided to APD staff related to Flock system users?

Training regarding our Flock system is incorporated into the formal training curriculum contained within each new officer's Field Training Program. As part of the field training process, a Field Training Officer (FTO) is required to evaluate and sign off on the trainee's knowledge and understanding of the Flock system. During field training, FTOs review the Flock system with trainees, including the requirements and provisions of the agency's ALPR policy. In addition, trainees are required to complete Flock Academy training, including the Search Clarification course and the User Training course. Upon completion, trainees receive certificates documenting successful completion of the courses.

Before an FTO signs off on the Flock section of the Phase One Field Training book, the trainee must demonstrate a working knowledge of the Flock system and an understanding of its proper use.

For current Flock users within the Auburn Police Department who did not previously complete the Flock Academy training described above, they are now required to complete the applicable courses and obtain a certificate of completion.

6. Is there updated training after Flock conducts a system update?

Relevant system updates are incorporated into the Flock Academy training videos.

7. Are we informed of a Flock system update in order to initiate training related to an update?

Administrators receive email notifications regarding relevant system activity and updates.

8. Can we get out of the contract tomorrow and at what cost?

The City's current agreement with Flock provides for an annual cost of approximately \$30,000 per year for the City's existing ALPR system. If the City continues the agreement through the end of the current June 2028 contract term, the City will continue to incur this annual expenditure through the expiration of the agreement.

If the City elects to terminate the agreement prior to the expiration of the contract term, the City would be subject to the applicable early termination provisions contained within the agreement. The contract currently provides that termination for convenience will result in a one-time fee of \$500 per Flock Hardware unit. Based on the City's current deployment of 12 Falcon cameras, the anticipated termination cost would be at least \$6,000, subject to confirmation from Flock regarding the contractual definition and calculation of "Flock Hardware."

9. What does misuse notification look like and who is notified?

Potential misuse is detected when an administrator is in the "Organization Audit" tab.

10. What safeguards or audits have been done to ensure the system is being used properly both by APD and by the outside agencies it's shared with?

- a. Audits every 30 days
- b. A reason for a search is a required field before a search can be conducted
- c. A case number or incident number is a required field before a search can be conducted
- d. Flock's Audit Assistance Feature – detects and notifies abnormal activity for APD administrators of the system to investigate
- e. Policy-driven and supported by a documented internal investigation into unexplainable repeat searches and other alleged misuses.

11. Is Flock compliant with California Law Enforcement Telecommunications System (CLETS) integration requirements?

Flock's system does not integrate with privileged information networks such as Department of Motor Vehicles, the FBI's National Crime Information Center, and

California's Automated Criminal History System, thus there is no cause for them to be compliant with CLETS.

The California Department of Justice reported that a private entity does not meet eligibility requirements to become a subscribing agency to receive privileged information. In other words, by not being eligible to receive privileged information from the above mentioned networks, there are no CLETS compliancy requirements.

12. What happens to Auburn's data once it "leaves" the city and is under Flock's own license and control?

Flock has stated, that once the City's data is deleted after the 30 day retention period, the Auburn Police Department and Flock are no longer able to access it.

13. Why is Auburn's data shared so extensively with NCRIC, and what happens to it once it reaches a federal fusion center?

Northern California Regional Intelligence Center's (NCRIC) core mission is to identify, prevent, and respond to human-made threats and major hazards in the Federal Northern District of California. Its key functions include:

- a. Intelligence Sharing & Analysis
- b. Threat Prevention & Mitigation
- c. Investigative Support
- d. Training & Preparedness
- e. Public Safety Collaboration

As noted above, NCRIC's goal is to conduct threat assessments and evaluate the likelihood of a threat being carried out within the State of California.

The center utilizes ALPR technology on a broader, statewide level rather than limiting its analysis to individual jurisdictions. This approach recognizes that threats do not necessarily remain within jurisdictional boundaries, as demonstrated by events such as September 11, 2001. By analyzing information on a broader scale, NCRIC is better positioned to identify patterns, connections, and potential threats that may otherwise go undetected when information is examined solely at the local level. This broader analysis may, in turn, assist in identifying threats that have a potential local impact.

NCRIC investigators complying with NCRIC CLETS mandates use the system as an investigative tool and practices a 30 day retention policy

14. There were noted concerns with violations of 4th Amendment rights; Pinal County, Arizona Sheriff Ross Teeple recently announced he will not renew his department's Flock contract when it expires this month — citing 4th Amendment concerns over the system's facial recognition and AI tracking capabilities — and made that call himself, simply informing his Board of Supervisors rather than waiting for their vote (<https://ktar.com/arizona-news/pinal-county-sheriff-flock-cameras-concerns>). Would Chief Morrison consider exercising that same discretion for Auburn PD, rather than making this contingent on a future Council vote?

It is important that the City Council is involved in the decision to allow the use, or prohibit the use, of this technology in the City. This provides a transparent process with an opportunity for community input.

15. Given that Flock's cameras and software have capabilities beyond what Auburn currently uses, and continue to gain new capabilities (and Auburn shares data with many other agencies and NCRIC), how can residents be confident those additional capabilities aren't being used without public knowledge? (For example, Sheboygan, WI recently canceled its Flock contract after discovering undisclosed data tracking: <https://www.fox6now.com/news/sheboygan-canceling-flock-contract-over-undisclosed-data-tracking>)

In the simplest terms, I believe this information could be captured through the Department's internal audit process and subsequently shared with the community to promote transparency and accountability.

16. Were any of the slides or data presented Monday night supplied by Flock, directly or indirectly? (We note Auburn's Transparency Portal is hosted on a flocksafety.com domain.)

Aside from the information contained in our Flock contract and the Auburn Police Department's Transparency Portal (as noted above), none of the slides, information, or data presented at the town hall meeting were supplied by Flock, either directly or indirectly.

17. As an AI system, what is the system's false-positive or misidentification rate, and what happens procedurally when the system flags an incorrect match?

At this time, there is not an efficient mechanism within the Flock platform for the Department to capture and quantify false-positive or misidentification rates. The City of Roseville was able to provide this information because it has personnel assigned to its Real-Time Crime Center who manually track and record this information.

The Department has submitted a client request to Flock asking that the platform include a “misread” designation or button for flagged vehicles, as well as the ability to generate a report identifying and tracking misreads.

Currently, when a Flock alert is determined to be a false positive or a misidentification, the information is communicated verbally between the dispatcher and patrol officer, or between the patrol officer and dispatcher. Once it is determined that the flagged vehicle or license plate is not a match, the alert is minimized on the computer screen, and the officer and dispatcher resume their normal duties.

The Department has also recently identified a function within the Flock platform that allows users to suppress a license plate that repeatedly registers as a misread. Staff are currently evaluating procedural options for effectively utilizing this function to reduce recurring false-positive alerts and improve the efficiency and accuracy of the system.



POLICY AND PROCEDURE

Subject:	Automated License Plate Readers (ALPRs) Usage and Privacy Policy	Index:	Health, Safety and Welfare
		Number:	403-1
Effective Date:	June 2, 2026	Prepared By:	Finance & Administrative Services
Supersedes:	N/A	Approved By:	City Council <i>[Signature]</i>

1.0 PURPOSE:

This policy provides guidelines for the use of Automated License Plate Reader (ALPR) technology and for the collection, use, storage, sharing, and protection of ALPR information and data by or on behalf of the CITY. This policy is intended to be consistent with California Civil Code §§ 1798.90.5–1798.90.55 and aligned with the Orange County Sheriff's Department (OCSd) ALPR policy. ALPR technology may be used by CITY personnel providing law enforcement services, CITY parking enforcement staff, and contractors or vendors authorized to operate ALPR systems on behalf of the CITY. This policy ensures that all such use is conducted in a lawful, transparent, and accountable manner, while respecting individuals' privacy and civil liberties.

2.0 ORGANIZATIONS AFFECTED:

All departments/divisions.

3.0 REFERENCES:

California Civil Code §§ 1798.90.5–1798.90.55; breach notification (California Civil Code § 1798.29); and Orange County Sheriff's Department ALPR Policy

4.0 POLICY OBJECTIVES:

This policy applies to all departments of the City of San Clemente (the City) where ALPR technology is used. It is the policy of the City of San Clemente to use ALPR

technology to enhance public safety, support law enforcement and parking enforcement operations, and assist with data-driven planning efforts, while protecting individual privacy and civil liberties. All ALPR use shall comply with applicable federal and state law and, where applicable, be consistent with OCSD policies and procedures.

5.0 ADMINISTRATION:

The City Manager or designee shall serve as the ALPR Program Manager and is responsible for ensuring compliance with this policy and applicable law. The Program Manager shall be responsible for system oversight and monitoring, coordination with OCSD, approval of vendors and contractors, ensuring required training, maintaining documentation and access logs, overseeing audits, monitoring the system for security and privacy compliance, ensuring data accuracy, and managing data retention/destruction. OCSD personnel using ALPR systems within the City shall operate in accordance with OCSD policy and procedures, which are incorporated fully by reference, and shall also comply with this policy where applicable. Any contractor or vendor operating ALPR systems on behalf of the City shall enter into a written agreement with the City and must maintain an ALPR usage and privacy policy compliant with California law and this policy. Every contractor policy must be reviewed and approved by the City prior to implementation and must not conflict with this policy.

6.0 USE OF ALPR SYSTEMS:

ALPR systems may be used in accordance with applicable law and for legitimate governmental purposes, including law enforcement, parking enforcement, and analytical applications such as parking, traffic, and mobility studies. Systems may be deployed in fixed or mobile configurations and used proactively or reactively to identify vehicles of interest and support enforcement and operational needs. ALPR alerts shall not, by themselves, constitute the sole basis for enforcement action. Prior to taking enforcement action, officers or authorized personnel shall independently verify ALPR information for accuracy and confirm the basis for contact through independent sources. Authorized users shall recognize that ALPR data, including associated hot lists, may not always be accurate. Users shall also visually confirm, to the fullest extent practicable, that the license plate and/or vehicle characteristics match the ALPR-generated image. ALPR systems shall only capture data from areas visible to the public where there is no reasonable expectation of privacy.

7.0 DATA COLLECTION:

ALPR systems shall collect only the data necessary to accomplish authorized purposes. Data collected shall include license plate images, plate numbers, date, time, and location of capture. Reasonable efforts shall be made to ensure data accuracy and system functionality.

8.0 AUTHORIZED USES:

ALPR data may be accessed and used only for legitimate governmental purposes, including law enforcement investigations, parking enforcement, locating stolen or

wanted vehicles, and approved analytical studies. Use of ALPR data shall be consistent with the purpose for which the data was collected and shall comply with all applicable laws.

9.0 PROHIBITED USES

ALPR systems and data shall not be used for purposes unrelated to official duties or in a manner that violates any law or constitutional right. ALPR data shall not be used to monitor individuals or groups based on protected characteristics or for personal, political, or commercial purposes.

10.0 DATA RETENTION

ALPR data shall be retained in accordance with California Civil Code §§ 1798.90.5–1798.90.55 and applicable City policy. Data not associated with an active investigation, enforcement action, booked as evidence, or legal hold shall not be retained longer than two (2) years. At the end of the retention period, data shall be automatically and securely deleted or destroyed using methods that prevent reconstruction, recovery or unauthorized access.

11.0 ACCESS AND SECURITY

Access to ALPR systems and data shall be restricted to Authorized Users with a legitimate operational purpose. Access approvals shall be reviewed at least annually. The City and all Authorized Users shall implement reasonable security procedures and practices to protect ALPR data from unauthorized access, disclosure, or misuse. All access to ALPR data shall be accessible through login/password-protected system capable of documenting all access by user identification, date, time, and purpose of access. Any breach of ALPR data shall be handled in accordance with Civil Code § 1798.29, including required notifications.

12.0 DATA SHARING

ALPR data may be shared only with another public agency for official purposes consistent with applicable law. All data sharing shall comply with California Civil Code §§ 1798.90.5–1798.90.55, Government Code § 7284.6 and any applicable agreements governing access and use. ALPR data shall not be sold, shared or transferred for personal, commercial, or other improper purposes. ALPR data may only be shared with a public agency that maintains a usage and privacy policy compliant with Civil Code § 1798.90.51, *et seq.*, and pursuant to a written agreement and established system access controls governing use, access, retention, and dissemination. Analytical uses may be provided to a non-public entity and shall be limited to aggregated or anonymized data, if feasible. All information and data sharing shall be logged by the City and subject to audit. The City may terminate access to or sharing of ALPR data due to noncompliance with any applicable law, restrictions, or this policy. Upon termination, contractors shall return or securely destroy all ALPR data and certify such destruction.

13.0 TRAINING

All Authorized Users shall complete training prior to accessing or using ALPR systems. Training shall include proper use, legal requirements, privacy

protections, civil liberties, data accuracy/verification, and system security. Contractors shall ensure that their personnel receive equivalent training.

14.0 ACCOUNTABILITY AND AUDIT

The City shall conduct annual audits and as may otherwise be needed to ensure compliance with this policy and applicable law. Audits shall include review of access logs, data queries, and system use, including sharing, retention, and accuracy compliance. OCSD audits may be relied upon for law enforcement use where applicable. Contractors shall be subject to City audit.

15.0 PUBLIC NOTICE AND TRANSPARENCY

The City shall maintain a written ALPR usage and privacy policy in accordance with California Civil Code §§ 1798.90.50–1798.90.55. The policy shall be made available to the public and posted on the City's website.

16.0 JOB TITLES/DESIGNATIONS OF AUTHORIZED USERS

Authorized users include, but are not limited to, sworn law enforcement officers, parking enforcement staff, code enforcement officers, designated analysts, and approved contractors, subject to training and approval by the ALPR Program Administrator.

17.0 CONTRACTORS AND THIRD PARTIES

Contractors or vendors using ALPR systems on behalf of the City shall comply with all provisions of this policy and applicable law. They must maintain a City-approved ALPR usage and privacy policy and implement appropriate safeguards for data security, retention and destruction.

18.0 VIOLATIONS

Any unauthorized access, use, retention/destruction or disclosure of ALPR data is prohibited and may result in disciplinary action (including termination of employment), termination of contract, civil liability, criminal prosecution, and/or other legal penalties.

19.0 MODIFICATIONS

Prior to implementation of significant modifications to the City's ALPR program or this policy, the City will provide an opportunity for public comment at a regularly scheduled meeting of the City Council, consistent with Civil Code § 1798.90.55(a). Minor changes to this policy or the City's ALPR program that are necessary to comply with applicable law, as it may be amended from time to time, may be approved and implemented by the City Manager in consultation with the City Attorney and shall be posted on the City's website.

20.0 DEFINITIONS:

(a) **ALPR System** – A system of cameras and computer software used to capture images of license plates and convert those images into computer-readable data.

(b) ALPR Data – Information or data collected through an ALPR system, including license plate numbers, images, date, time, and location.

(c) Authorized User – Any individual authorized by the City, OCSD, or an approved contractor to access or use ALPR systems or data.

(d) Hot List – A list of license plates associated with vehicles of interest, including stolen vehicles, wanted persons, or investigative alerts.

E□□I□IT “A”

City of Carson

Automatic License Plate Reader Usage and Privacy Policy

California Civil Code Section 1798.90.51 requires public agencies operating Automatic License Plate Readers (“ALPR” or “ALPRs”) to adopt and implement a usage and privacy policy in order to ensure that the collection, use, maintenance, sharing, and dissemination of information collected pursuant to such system protects individual privacy and civil liberties. Consistent with the state law mandate, the City of Carson (“City”) has adopted this Automatic License Plate Reader Policy (“Policy”) to regulate the use, management, retention and other aspects of the City’s ALPRs, ultimately for the purpose of deterring criminal activity and to aid law enforcement in its investigation and prosecution of possible crimes. This Policy shall be made available to the public in writing and posted on the City’s website.

The City operates ALPRs which are automatic license plate recognition camera systems that collect clear vehicle plate, make, model, color and speed data that will help the City, through the Los Angeles County Sheriff’s Department (“LASD”), capture critical investigative data and protect its citizens within certain strategically placed locations within the City, including within public rights of way and entrances to City facilities. The ALPR system is a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of license plates and the characters they contain into computer-readable data (“ALPR Data”).

- 1. The purpose of this Policy is to set forth the procedures for use of the ALPRs and ALPR Data conducted and collected in the course and scope of LASD providing law enforcement and crime prevention services as well as establishing use and data retention policies. The City will only make the ALPR Data available to the following: (1) LASD, which provides law enforcement services for the City, in accordance with LASD’s duly adopted policy and procedures, and (2) other law enforcement or prosecutorial agencies upon request from those agencies. Authorized Purposes for Using the License Plate Cameras and Collecting Photographic License Plate Images and/or ALPR Data.**

The purpose for using ALPRs and collecting ALPR Data is to deter criminal activity and to aid law enforcement in its investigation and prosecution of possible crimes.

Any data obtained from the City’s ALPRs shall be used and handled pursuant to this Policy, LASD policy, the policies of law enforcement or prosecutorial agencies that request ALPR Data, and applicable state and federal law. All other uses not referenced above shall be prohibited. ALPR Data should under no circumstances be used for personal purposes or purposes not specifically authorized herein. Possession of ALPR Data does not negate the need to comply with other laws or regulations including the requirement to obtain a search warrant when legally required.

2. Persons Authorized to Access the Cameras or Collect License Plate Image/ALPR Data.

The ALPRs are installed and maintained by an independent contractor using proprietary technology. All ALPR Data is sent directly to LASD and securely stored in a cloud-based server where all data (both footage and metadata) is fully encrypted and automatically deleted after five (5) years. The ALPR system shall only be accessed by sworn LASD officers in accordance with applicable policy and procedures duly adopted by LASD. The independent contractor shall not access footage without explicit, written permission from the City to help collect evidence in the event of a crime and shall not share, sell, or monetize ALPR Data. The independent contractor shall be responsible for maintaining the ALPRs.

3. Training.

Training on the use of ALPRs shall be provided by the independent contractor as needed by LASD. The basic ALPR software interface is intuitive and specific queries can only be done after all the information is collected, including search purposes and identifying information as to the individual conducting the search. There are also detailed help tutorials within the basic ALPR software to assist with helping each user to run certain basic queries.

4. How the License Plate Cameras will be monitored to Ensure Security of the Information and Compliance with Applicable Privacy Laws.

ALPR Data is confidential and shall not be shared or open to the public for review. ALPR Data may only be shared with LASD personnel in accordance with LASD's duly adopted policy, and other law enforcement or prosecutorial agencies for official law enforcement purposes in accordance with this Policy and the policies adopted by such agencies. Data shall not be used for any non-work-related purposes and all uses shall take into consideration the privacy, civil rights, and civil liberties of individuals.

All information collected and stored as part of the ALPR system, including photographic license plate images and/or ALPR Data shall be closely safeguarded and protected by both procedural and technological means and shall be securely stored in a secured cloud-based server.

5. The purposes of, process for, and restrictions on, the sale, sharing, or transfer of license plate image data to other persons.

All ALPR Data are stored only on the secured cloud-based server. The stored data shall only be accessed by LASD or other law enforcement agency when requested by the agency as part of a criminal investigation. The LASD shall maintain a log or other system that shows, at minimum, (1) the date any data was accessed by LASD or requested and provided to any other agency, (2) which agency accessed or was provided the data, (3) the license plate number or other data elements used to query the ALPR system, (4)

the username of the person who accessed the information and, as applicable, the organization or entity with whom the person is affiliated, and (5) the purpose for accessing the information. All ALPR Data access requires a username and password for access.

Once photographic license plate images and/or ALPR Data is obtained by a law enforcement agency, it shall become the property of that agency, and the City of Carson shall have no responsibility for that data and shall not be required to maintain any copy thereof. Moreover, the usage and privacy policies of that agency will apply.

6. The Title of the Official Custodian, or Owner, of the License Plate Cameras responsible for implementing this Policy.

The Assistant City Manager or City Manager's designee shall be responsible for implementing this Policy.

7. A Description of the Reasonable Measures that will be used to ensure the Accuracy of License Plate Camera Data and Correction of Data Errors.

The independent contractor shall, no less than once every thirty (30) days, monitor the ALPR system including data storage to ensure that the system is working properly. If any portion of the system is found to be working improperly, the independent contractor shall take all reasonable measures to timely correct any problem. The independent contractor shall maintain a log or other system that records when a problem was discovered, and the time period, if any, that the system was not working or not working properly.

The ALPR system shall be monitored and maintained by the independent contractor to ensure functionality, reliability and functionality in accordance with specific terms and conditions of the applicable agreement.

8. The Length of Time the License Plate Image Data Will be Retained, and the Process Utilized to Determine if and when to Destroy Data.

Data from the APLR system including all ALPR Data that is collected by the independent contractor shall be stored for period of five (5) years from the date of recordation of the data. The ALPRs will be set/programmed for a five (5) year retention period after which time ALPR Data will be permanently deleted one minute after such data retention period has expired.

9. Security Procedures to Protect License Plate Image and ALPR Data.

The independent contractor shall maintain reasonable security procedures including operational, administrative, technical, and physical safeguards to protect license plate image data from unauthorized access, destruction, use, modification, or disclosure.

10. Notice of Breach of Security.

In the event of a breach of security of license plate image data, the City will provide notice of said breach pursuant to Civil Code section 1798.29.

RESOLUTION NO. 24-094

A RESOLUTION OF THE CUPERTINO CITY COUNCIL ESTABLISHING A POLICY FOR AUTOMATED LICENSE PLATE READERS

WHEREAS, Automated License Plate Reader (ALPR) cameras are used by police departments across the United States to instantly capture license plate information and compare it against lists of license plates associated with stolen vehicles, people who have committed a crime, and for other investigative purposes; and

WHEREAS, many organizations that have used ALPR technology have found it to be an effective tool in fighting crime; and

WHEREAS, California Civil Code section 1798.90.5 requires that public agencies with ALPRs adopt and implement a usage and privacy policy that identifies the individuals who will have access to the ALPR data, describes how the ALPR system will be monitored, lists parameters for sharing of ALPR data, describes measures that will be taken to protect the accuracy of ALPR data, and specifies the retention period for ALPR data.

NOW, THEREFORE, BE IT RESOLVED that the City Council of the City of Cupertino hereby adopts the attached Automated License Plate Reader Policy for the use of ALPR cameras in the City of Cupertino.

PASSED AND ADOPTED at a regular meeting of the City Council of the City of Cupertino this 1st day of October, 2024, by the following vote:

Members of the City Council

AYES: Mohan, Fruen, Chao, Moore
 NOES: None
 ABSENT: Wei
 ABSTAIN: None

SIGNED: <u>Sheila Mohan</u> Sheila Mohan, Mayor City of Cupertino	<u>10/10/2024</u> Date
ATTEST: <u>Kirsten Squarcia</u> Kirsten Squarcia, City Clerk	<u>10/10/2024</u> Date

CITY OF CUPERTINO AUTOMATED LICENSE PLATE READER POLICY

I. Purpose

The City of Cupertino ("City") leases an Automated License Plate Reader (ALPR) system within the City operated by the Santa Clara County Sheriff's Office ("Sheriff's Office") for certain law enforcement and public safety purposes. ALPR systems use high-speed cameras to photograph vehicle license plates. The City intends to contract with vendors to install and maintain the ALPR system. The City ALPR system may also obtain data from ALPR cameras not owned or leased by the City. This policy applies to data held within the City's ALPR system but does not apply to data held independently by the owners or lessors of ALPR cameras not owned or leased by the City. The City ALPR system is intended only for authorized law enforcement and public safety purposes, and its data are only intended to be accessed by authorized users.

California Civil Code section 1798.90.5 requires public agencies operating ALPR systems to adopt and implement a usage and privacy policy to ensure that the collection, use, maintenance, sharing, and dissemination of information collected pursuant to such system protects individual privacy and civil liberties. Consistent with the City's commitment to individual privacy and civil liberties and the State law mandate, the City has adopted this policy to regulate the use, management, retention, and other aspects of the City's ALPR system. This policy shall be made available to the public in writing and posted on the City's website.

II. Authorized and Prohibited Uses

The City ALPR system shall only be utilized for the following purposes:

- To locate stolen, wanted, and/or other vehicles that are the subject of an investigation
- To locate and/or apprehend individuals subject to arrest warrants or who are otherwise lawfully sought by law enforcement
- To locate victims, witnesses, suspects, and others associated with a law enforcement investigation
- To locate missing persons, including in response to Amber Alerts and Silver Alerts
- To support local, State, Federal, and regional public safety departments in the identification of vehicles associated with targets of criminal investigations,

- including investigations of serial crimes
- To analyze traffic patterns using anonymized data
- To protect participants at special events; and
- To protect critical infrastructure sites.

Any data obtained from the City ALPR system shall be used and handled pursuant to this policy and applicable State and Federal law. All other uses not referenced above are prohibited. Under no circumstances shall the ALPR system be used for personal or commercial purposes or other purposes not specifically authorized above. Access to the ALPR system does not negate the need to comply with other laws or regulations, including obtaining a search warrant when legally required. The City shall at no time maintain an account for the ALPR system that allows the City to access the data collected or stored by the ALPR system.

III. Data Collection

The City ALPR system shall collect digital images of vehicle license plates and their associated license plate numbers. The ALPR system shall collect the date and time the license plate passes a digital-image site where an ALPR is located, a captured vehicle's geographical location, and vehicle details (make, model, type, and color). Live video, vehicle speeds, and audio shall not be provided or recorded. To the extent practicable, the ALPR system shall be designed to blur images of individuals that the system may inadvertently collect.

IV. Installation and Maintenance

This policy addresses the installation and maintenance of city-owned or leased ALPR devices. An Encroachment Permit will be required for the installation of these devices. While there will be no fee for the permit, an insurance certificate will be necessary. A traffic control plan will also be required if traffic is obstructed during installation.

No privately leased or owned ALPR devices will be permitted on City infrastructure. The City will lease the ALPR devices from a vendor responsible for installation and maintenance. The vendor will not be authorized to access data collected by the ALPR system under any circumstances. Their role will be limited to operating, inspecting, troubleshooting, and maintaining the system hardware, software, associated cloud storage mechanisms, and servers, as necessary. To the extent feasible, cameras should be directed toward public property and away

from private property.

V. Data Access, Storage, and Protection

The City's ALPR system may only be used by, and data collected thereunder shall be accessible only by, personnel of the Sheriff's Office pursuant to a contract providing law enforcement services to the City. The City's ALPR system shall be accessible only through a login and password-protected system capable of documenting individual user access by name, date, and time.

In addition to this policy, Sheriff's Office personnel shall observe and comply with the Sheriff's Office Surveillance Use Policy and any additional guidelines and regulations that are in place governing ALPR use and access. Prior to the City granting use and access, the Sheriff's Office shall execute an agreement with the City and/or the City's contracted ALPR vendor(s), to the satisfaction of the City Attorney, agreeing to comply with this policy.

Contracts with vendors for the operation, maintenance, and repair of the ALPR system shall provide that the vendor is not authorized to access data collected by the ALPR system under any circumstances. Such vendors shall only be tasked with operating, inspecting, troubleshooting, and maintaining the system hardware, software, associated cloud storage mechanisms, and servers, as necessary.

Data collected by the City ALPR system is automatically uploaded to the ALPR system's associated cloud storage at the time of capture. The City's contracted ALPR vendor shall provide and maintain cloud storage and server capacity as part of the scope of services. The City shall confirm that the contracted vendor installs and implements appropriate security measures for such storage, including encryption, firewalls, authentication, and other reasonable data protection measures.

Data stored in the City ALPR system cloud space shall not be downloaded to a local server, stored locally on a hard drive or portable device, or provided in a physical printout, except in the following cases:

- Where the ALPR system has identified vehicle license plate images and numbers as a match to a law enforcement registry
- Where data retrieval is necessary for conducting or assisting with a criminal investigation or to facilitate an authorized use identified in Section II

above

Only personnel from the Sheriff's Office working in an investigative or enforcement function may download ALPR data for local storage or printout (collectively, "Local Data") for authorized purposes stated herein. Data from the City ALPR system may not otherwise be downloaded for any other purpose, whether by Sheriff's Office authorized personnel, City staff, or other individuals or entities.

Local Data shall be maintained in accordance with applicable State and Federal evidentiary laws and in accordance with appropriate chain of custody practices. Additionally, the Sheriff's Office shall implement physical security, encryption, firewalls, authentication, and other reasonable security measures to protect Local Data retrieved from the system.

Local Data shall be accessible only through a login and password-protected system capable of documenting individual user access by name, date, and time.

VI. Data Retention

Data stored in the ALPR cloud system shall be purged after thirty (30) days from the date it was uploaded to the cloud system unless downloaded or stored pursuant to Section IV above.

Data that is downloaded or stored pursuant to Section IV above shall be purged no later than twelve (12) months from the date it was downloaded for local storage unless the data thereafter becomes associated with a criminal investigation or an ongoing case for an authorized purpose identified in Section II above. In the latter case, the data shall be retained for the duration of the criminal investigation and the criminal proceedings through adjudication of the case in the same manner as other evidence in the matter unless otherwise ordered by the court to be retained for a longer period or permanently.

VII. Public Access

Data from the City ALPR system shall not be sold, shared, or transferred except as explicitly authorized by this policy. Data from the City ALPR system shall not be made public unless specifically required by State or federal law or court order. If a public request for data is received, the Sheriff's Office shall consult with the Santa Clara County Counsel's Office to determine whether the requested data is exempt

from disclosure pursuant to the California Public Records Act or other State or Federal law provisions, and whether any additional steps are required in response to such a request for data.

VIII. Third-Party Data Sharing

Data-sharing from the City's ALPR system shall be limited to only the following:

- District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence
- Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with California criminal discovery laws; and
- Other law enforcement agencies, as part of a formal criminal or administrative investigation
- Parties to civil litigation in response to a court order.

IX. Training

All personnel authorized to use and access the ALPR system and data pursuant to this policy shall receive all required training from the Sheriff's Office. Said personnel shall also review and receive copies of this policy and the Sheriff's Office Surveillance Use Policy.

X. Oversight

The Sheriff's Office shall ensure compliance with this policy as the provider of law enforcement services to the City.

All-access to ALPR system data shall be logged, and the Sheriff's Office shall maintain an audit trail of requested and accessed information, including the purpose of the search. Periodic, random audits shall be conducted by the Sheriff's Office and on at least an annual basis. Audits shall ensure compliance with this policy and all applicable laws and shall be used to ensure the accuracy of ALPR information and correct data errors. Audit reports shall contain at least the following information:

- Name of law enforcement agency that accessed the data
- Date and time of access

- Reason for accessing data
- Activity executed, including any license plate numbers searched identified in a separate confidential appendix
- Incident number associated with the investigation
- The number of arrests resulting from the ALPR system
- The number and type of data requests, disclosures, and denials
- The number and nature of any violations of this policy or applicable laws
- The number and resolution of any complaints received
- Any challenges or problems encountered with the ALPR system
- Any recommendations for improvement or enhancement of the ALPR system

Upon completion of each audit, the Sheriff's Office shall provide a copy of the audit report to the City Manager or the City Manager's designee within five (5) business days of completion.

**MEMORANDUM OF UNDERSTANDING BETWEEN THE COUNTY OF SANTA
CLARA AND THE CITY OF CUPERTINO REGARDING THE USE OF AUTOMATIC
LICENSE PLATE READERS (ALPRs)**

This Memorandum of Understanding ("MOU") is made between the County of Santa Clara ("County") and the City of Cupertino ("City") (collectively referred to as the "Parties" and each one a "Party") regarding the administration of the City's Automatic License Plate Reader system ("ALPRs").

I. PURPOSE

In 2014, the County entered into a Law Enforcement Contract with the City pursuant to which the County of Santa Clara Office of the Sheriff ("Sheriff's Office") provides law enforcement services within the corporate limits of the City. In 2024, the Parties entered into a First Amendment to the Law Enforcement Contract. The Law Enforcement Contract and the First Amendment to the Law Enforcement Contract are attached as Exhibit A to this MOU.

The City has acquired ALPRs for use within the corporate limits of the City.

The City desires that the Sheriff's Office administer the ALPR system pursuant to the Law Enforcement Contract and the First Amendment to the Law Enforcement Contract between the County and the City.

The purpose of this MOU is to govern the Parties' obligations with respect to the ALPRs.

II. ROLES AND RESPONSIBILITIES

A. Acquisition and Maintenance of ALPRs

The City will be responsible for the acquisition, installation, and maintenance of the ALPRs, and any associated costs. The City may consult with the Sheriff's Office on the placement of the ALPRs.

B. Authorized and Prohibited Uses

The ALPRs will only be used for the purposes identified in the City's ALPR Policy (attached as Exhibit B) and the County ALPR Surveillance Use Policy (attached as Exhibit C). Where a conflict exists between the City ALPR Policy and the County ALPR Surveillance Use

Policy, the more restrictive policy shall govern the conduct of the County and the Sheriff's Office, and any officers, employees, or agents thereof, with respect to the ALPRs.

C. Data Collection, Storage, Access, Sharing, and Retention

Data collection, storage, access, sharing, and retention will be in accordance with the City ALPR Policy and the County ALPR Surveillance Use Policy. Where a conflict exists between the City ALPR Policy and the County ALPR Surveillance Use Policy, the County ALPR Surveillance Use Policy shall govern the conduct of the County and the Sheriff's Office, and any officers, employees, or agents thereof, with respect to the ALPRs.

The City further agrees that it will delegate the administrative account with two-factor authentication enabled for the ALPR system to a Sheriff's Office employee designated by the Sheriff's Office. The City shall at no time maintain an account for the ALPR system that allows the City access to the data collected or stored by the ALPR system.

D. Data Ownership

As between the County and the City, the City owns the images captured by the ALPR system. The County owns any data input by the Sheriff's Office into the ALPR system and any data or records generated by the ALPR system or by the ALPR vendor reflecting a match between an image and a vehicle of interest.

E. Training

All Sheriff's Office personnel authorized to use and access the ALPR system and data pursuant to this MOU shall receive all required training from the Sheriff's Office. Said Personnel shall also review and receive copies of the City ALPR Policy and the County ALPR Surveillance Use Policy.

F. Oversight

Each Party will ensure that its officers, employees, and agents comply with this MOU, including the City ALPR Policy and County Surveillance Use Policy.

All access to ALPR Data shall be logged, and the Sheriff's Office shall maintain an audit trail of requested and accessed information, including the purpose of the search. The

Sheriff's Office shall conduct an audit on at least an annual basis to determine compliance with this MOU, the incorporated exhibits, and all applicable laws. The Sheriff shall provide copies of the audit report to the City as requested but is entitled to withhold any law enforcement-sensitive portions of the report (e.g., California Department of Justice or other criminal justice data released on a need-to-know/right-to-know basis).

G. Compensation

The Sheriff's Office will be compensated for services performed under this MOU in accordance with the Law Enforcement Contract and the First Amendment to the Law Enforcement Contract.

III. TERM OF AGREEMENT

The term of this MOU shall commence upon the date of execution by all Parties and shall expire on June 30, 2026, unless otherwise terminated by the Parties as provided herein. The Parties may extend the term of the MOU by written amendment to this MOU executed by all Parties.

IV. TERMINATION

Any Party may terminate this MOU, at any time and without cause, upon 60 days' written notice given to the other Party pursuant to Section VI, "NOTICES."

The County (through the Board of Supervisors) may immediately terminate the MOU for cause if it determines that the City is violating the terms of this MOU, including the attached Exhibits. Prior to terminating for cause, the County must provide the City with notice of the alleged breach and provide the City 5 business days to respond and remedy the breach. The County (through the Board of Supervisors) may immediately terminate the MOU if City fails to timely remedy the breach.

Notwithstanding Section III, the MOU shall immediately terminate upon the termination of the Law Enforcement Contract (including any extensions or amendments thereof).

Should the City revoke or amend the City ALPR Policy or the County revoke or amend the County ALPR Policy, either Party has the option to either terminate this MOU or to offer

an amendment to the MOU.

V. AMENDMENTS

This MOU may only be amended by a written instrument signed by the Parties.

VI. NOTICES

Any notice required to be given under this MOU shall be in writing and addressed as follows:

Notice to County:

Robert Jonsen, Sheriff
Santa Clara County Office of the Sheriff
55 W. Younger Avenue
San Jose, CA 95110

County of Santa Clara Board of Supervisors
70 West Hedding Street
East Wing, 10th Floor
San Jose, CA 95110

James Williams, County Executive
70 West Hedding Street
11th Floor
San Jose, CA 95110

Tony LoPresti, County Counsel
70 West Hedding Street
East Wing, 9th Floor
San Jose, CA 95110

Notice to City:

Pamela Wu, City Manager
10300 Torre Avenue
Cupertino, CA 95014

Christopher Jensen, City Attorney
10300 Torre Avenue
Cupertino, CA 95014

Thomas Chin, Emergency Manager
10300 Torre Avenue
Cupertino, CA 95014

The notice required by this MOU shall be effective when, according to timestamps in the sender's email system or deposited in the United States mail, first-class postage is prepaid.

VII. INDEMNIFICATION AND INSURANCE

Indemnification and insurance for purposes of this MOU will be governed by Sections IV and V of the Law Enforcement Contract.

VIII. RECORDS REQUESTS

The Parties are public agencies subject to the disclosure requirements of the California Public Records Act ("CPRA").

To the extent a Party's proprietary information is contained in documents or information submitted to any other Party, and the Party submitting the document or information ("submitting Party") claims that such information falls within one or more CPRA exemptions, the submitting Party must clearly mark such information "CONFIDENTIAL AND PROPRIETARY" or with similar language, and identify the specific lines containing the information. In the event of a request for such information, the Party in receipt of such information ("receiving Party") will make best efforts to provide notice to the submitting Party prior to such disclosure pursuant to a CPRA request. If the receiving Party receives a CPRA request seeking or partially seeking information clearly marked as confidential or proprietary of the submitting Party, the receiving Party will provide written notice to the submitting Party in a reasonably prompt manner. If the submitting Party contends that any documents are exempt from the CPRA and wishes to prevent disclosure, it is required to obtain a protective order, injunctive relief or other appropriate remedy from a court of law in Santa Clara County before the receiving Party is required to respond to the CPRA request. If the submitting Party fails to obtain such remedy within the time the receiving Party is required to respond to the CPRA request, the receiving Party may disclose the requested information.

Data collected by the ALPRs shall not be made public unless required by federal or state law or court order. The Parties agree that they will notify and consult with the other

with respect to any CPRA request seeking records relating to the ALPR system.

The Parties agree that it shall defend, indemnify, and hold harmless the other against any claim, action or litigation (including but not limited to all judgments, costs, fees, and attorneys' fees) that may result from denial of a CPRA request for information arising from any representation, or any action (or inaction) of the indemnifying Party.

IX. CONFLICTS OF INTEREST

The Parties shall comply, and shall ensure that their employees, contractors and subcontractors comply, with all applicable (i) requirements governing avoidance of impermissible client conflicts; and (ii) federal, state and local conflict of interest laws and regulations including, without limitation, California Government Code section 1090 et. seq., the California Political Reform Act (California Government Code section 87100 et. seq.) and the regulations of the Fair Political Practices Commission concerning disclosure and disqualification (2 California Code of Regulations section 18700 et. seq.). In accepting this MOU, the Parties covenant that they presently have no interest, and will not acquire any interest, direct or indirect, financial or otherwise, which would conflict in any manner or degree with the performance of this MOU. Each Party is responsible for assuring compliance of its subcontractors and employees with the requirements of this provision.

X. NON-DISCRIMINATION

The Parties shall comply with all applicable laws concerning nondiscrimination and equal opportunity in employment and contracting, including but not limited to the following: Title VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act of 1990; the Age Discrimination in Employment Act of 1967; the Rehabilitation Act of 1973 (Sections 503 and 504); the Equal Pay Act of 1963; California Fair Employment and Housing Act (Gov. Code § 12900 et seq.); California Labor Code sections 1101, 1102, and 1197.5; and the Genetic Information Nondiscrimination Act of 2008. In addition to the foregoing, the Parties shall not discriminate against any subcontractor, employee, or applicant for employment because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical

condition, political belief, organizational affiliation, or marital status in the recruitment, selection for training (including but not limited to apprenticeship), hiring, employment, assignment, promotion, layoff, rates of pay or other forms of compensation. Nor shall the Parties discriminate in the provision of services provided under this contract because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status.

XI. GOVERNING LAWS AND VENUE

This MOU has been executed and delivered in, and shall be construed and enforced in accordance with, the laws of the State of California. The proper venue for legal action regarding this MOU shall be in Santa Clara County.

XII. ENTIRE AGREEMENT

This MOU and its Exhibits and/or Attachments constitute the final, complete, and exclusive statement of the terms of the agreement between the Parties regarding the subject of this MOU. All Exhibits and/or Attachments to this MOU are incorporated herein as one agreement. This MOU incorporates and supersedes all the agreements, covenants and understandings between the Parties concerning the subject matter hereof, and all such agreements, covenants and understandings have been merged into this MOU. In the event that any term, condition, provision, requirement, or specification set forth in the body of this MOU conflicts with or is inconsistent with any term, condition, provision, requirement, or specification in any Exhibit and/or Attachment to this MOU, the provisions of the body of the MOU shall prevail. No prior or contemporaneous agreement or understanding, verbal or otherwise, of the Parties or their agents shall be valid or enforceable unless embodied in this MOU.

XIII. THIRD PARTY BENEFICIARIES

This MOU does not, and is not intended to, confer any rights or remedies upon any person or entity other than the Parties.

XIV. SIGNATORIES NOT AGENTS/INDEPENDENT CONTRACTOR

Parties to this MOU shall have no authority, express or implied, to act on behalf of any

signatory in any capacity whatsoever as an agent. The Parties shall have no authority, express or implied, pursuant to this MOU to bind each other to any obligation whatsoever. This MOU is not a contract of employment and does not create an employer-employee relationship between the Parties and neither Party shall be considered the employees of the other and shall not qualify for or become entitled to any claims for employment and retirement benefits from the other.

XV. NON-ASSIGNMENT

No assignment of this MOU or of the rights and obligations hereunder shall be valid without the prior written consent of all Parties.

XVI. WAIVER

No delay or failure to require performance of any provision of this MOU shall constitute a waiver of that provision as to that or any other instance. Any waiver granted by a party shall be in writing and shall apply to the specific instance expressly stated.

XVII. COUNTERPARTS

This MOU may be executed by the Parties in separate counterparts, each of which, when so executed and delivered, shall be an original, but all such counterparts shall together constitute one and the same instrument.

XVIII. CONTRACT EXECUTION

Unless otherwise prohibited by law or County or City policies, the Parties agree that an electronic copy of a signed contract, or an electronically signed contract, has the same force and legal effect as a contract executed with an original ink signature. The term "electronic copy of a signed contract" refers to transmission by facsimile, electronic mail, or other electronic means of a copy of an original signed contract in a portable document format. The term "electronically signed contract" means a contract executed by applying an electronic signature using technology approved by the County or the City.

XIX. COVID-19 REQUIREMENTS (IF APPLICABLE)

City shall comply with all County requirements in effect relating to COVID-19 for persons who routinely perform services for County onsite and share airspace with or

proximity to other people at a County facility as part of their services for County as set forth in a County Health Order (or similar directives) available at <https://covid19.sccgov.org/home>, and incorporated herein by this reference. City shall comply with all reasonable requests by County for documentation demonstrating City's compliance with this Section.

XX. LEVINE ACT COMPLIANCE

City will comply, and will ensure that its agents (as that term is defined under 2 Cal. Code Regs. § 18438.3(a)) and its subcontractors identified in City's proposal responding to a County solicitation and/or identified in this Agreement ("Subcontractors") comply, with California Government Code section 84308 ("Levine Act") and the applicable regulations of the Fair Political Practices Commission concerning campaign disclosure (2 California Code of Regulations sections 18438.1 – 18438.8), which (1) require a party to a proceeding involving a contract to disclose on the record of the proceeding any contribution, as defined by Government Code section 84308(a)(6), of more than \$250 that the party or their agent has made within the prior 12 months, and (2) prohibit a party to a proceeding involving a contract from making a contribution, as defined by Government Code section 84308(a)(6), of more than \$250 to any County officer during the proceeding and for 12 months following the final decision in the proceeding. City agrees to submit any disclosures required to be made under the Levine Act at the Office of the Clerk of the Board of Supervisors website at <http://www.sccgov.org/levineact>, and Contractor shall require Subcontractors to do the same. If this Agreement is to be considered or voted upon by the County's Board of Supervisors, City shall complete the Levine Act Contractor Form: Identification of Subcontractors and Agents, and if applicable, shall ensure that any Subcontractor completes the Levine Act Subcontractor Form: Identification of Agents, and City must submit all such forms to the County as a prerequisite to execution of the Agreement.

IN WITNESS WHEREOF, the Parties have caused the Agreement to be executed as of the Effective Date written above.

COUNTY OF SANTA CLARA

CITY OF CUPERTINO

Susan Ellenberg
President, Board of Supervisors

Date: _____

Pamela Wu
City Manager

Date: _____

Signed and certified that a copy of this document
has been delivered by electronic or other means to
the President, Board of Supervisors.

APPROVED AS TO FORM AND LEGALITY:

APPROVED AS TO FORM AND LEGALITY:

Stephanie M. Jackson
Deputy County Counsel

Date: _____

Christopher D. Jensen
Cupertino City Attorney

Date: _____

ATTEST:

ATTEST:

Curtis Boone
Acting Clerk of the Board

Date: _____

Kirsten Squarcia
City Clerk

Date: _____

CHAPTER 9 AUTOMATIC LICENSE PLATE READERS

§ 4-9.01. Purpose and applicability.

This chapter applies to those automatic license plate readers (ALPRs) that are either owned or contracted for by the Town and deployed at fixed locations in Los Altos Hills for the purposes of deterring crime, assisting with law enforcement investigations, and creating a safer environment for the Los Altos Hills community. The purpose of this chapter is to ensure that the collection, use, maintenance, sharing, and dissemination of information collected pursuant to ALPRs owned or contracted for by the Town protect individual privacy and civil liberties, and also to enforce regulations regarding the use, management, retention and other aspects of Town ALPRs.

(§ 2, Ord. 595, September 18, 2021)

§ 4-9.02. Definitions.

ALPR policy means a City Council-adopted and publicly available policy of the Town governing the use, operation, management, data retention and other aspects of ALPRs.

Authorized personnel means individuals or entities that are authorized to access data collected by ALPRs pursuant to an ALPR policy.

Automatic license plate reader or ALPR means the technology, software and hardware owned or contracted for by the Town and deployed in Los Altos Hills that provide automated detection of vehicle license plates using high speed cameras or other similar means.

Data means any and all information gathered by ALPRs in the form of license plates and metadata (such as location and time of the license plates being viewed), as well as access records, searches, and any other operational data collected by the ALPR software system used to store, index, and access the information gathered by ALPRs.

(§ 2, Ord. 595, September 18, 2021)

§ 4-9.03. Regulations pertaining to operations and data use.

Only authorized personnel may operate and access ALPR systems and data collected thereunder. The Town shall develop, and the City Council shall adopt and may amend from time to time, an ALPR policy that establishes the requirements and standards governing the use, operation, maintenance, and data collection and access for Town ALPRs. The ALPR policy shall also impose requirements relating to the collection, use, maintenance, sharing, and dissemination of information collected pursuant to ALPRs. The ALPR policy shall be made available to the public in writing and posted on the Town's website.

(§ 2, Ord. 595, September 18, 2021)

§ 4-9.04. Penalties for violation.

- (a) Any person violating the Council-adopted ALPR policy, as may be amended from time to time, is guilty of a misdemeanor pursuant to Municipal Code Section 1-2.06

§ 4-9.04

§ 4-9.04

and shall be subject to a fine of \$1,000. Violations of the ALPR policy shall include, but are not limited to, unauthorized access, possession, or release of data and information gathered or stored by ALPRs.

- (b) In addition, violations of this chapter shall be subject to any administrative, civil, or criminal enforcement remedies available under the law and/or the Municipal Code including cost recovery provisions under Section 1-2.04. The Town may enforce the violation of this chapter by means of civil enforcement through a restraining order, a preliminary or permanent injunction or by any other means authorized by law. Where it is necessary for the Town to file a civil action in court to obtain compliance with this chapter, the court may, in its discretion, assess a civil penalty based on factors outlined in Municipal Code Section 1-2.05(a) against the violating parties in the event the Town is the prevailing party.
- (c) Each violation shall be deemed a distinct and separate offense.
- (d) In accordance with Civil Code Section 1798.90.54, an individual who has been harmed by a violation of this chapter, including, but not limited to, unauthorized access or use of ALPR information or a breach of security of an ALPR system, may bring a civil action in any court of competent jurisdiction against a person who knowingly caused the harm. The court may award a combination of any one or more of the following:
 - (1) Actual damages, but not less than liquidated damages in the amount of \$2,500.
 - (2) Punitive damages upon proof of willful or reckless disregard of the law.
 - (3) Reasonable attorney's fees and other litigation costs reasonably incurred.
 - (4) Other preliminary and equitable relief as the court determines to be appropriate.

(§ 2, Ord. 595, September 18, 2021)



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.



Automatic License Plate Reader Privacy Model Bill

Section 1. Definitions.

- (A) “Automatic License Plate Reader (ALPR) system” shall mean a system, software, or computer algorithm, whether used independently or in combination with one or more mobile or fixed automated cameras, that is used to convert images of license plates into computer-readable data.
- (B) “Captured plate data” shall mean the GPS coordinates, date and time, photograph, license plate number, and any other data captured by, derived, or inferred from any automatic license plate reader system, including but not limited to make, model, color, and other vehicle-related characteristics.
- (C) “Government entity” shall mean a department or agency of the state of [insert State name] or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.
- (D) “Hot list” shall mean a database of compiled license plate and other vehicle identifying information, which is maintained in a manner that ensures it is and remains accurate, relevant, timely, and complete, that reflects a law enforcement-related, government entity’s determination that a vehicle or an individual associated with a vehicle is relevant and material to an ongoing criminal or missing persons enforcement effort or investigation.
- (E) “Secured area” shall mean an area, enclosed by clear boundaries, to which access is limited and not open to the public and entry is only obtainable through specific access-control points.

Section 2. Restrictions on use.

- (A) Except as provided for in Section 2(B), it shall be unlawful for any government entity to operate or use an automatic license plate reader system or the data therefrom.
- (B) An automatic license plate reader system and the data therefrom may be operated or used by a government entity only:
 - (1) For the comparison of captured plate data with hot list data to determine if a vehicle scanned by an ALPR system is relevant and material to an investigation of a vehicle that is:
 - (a) Unregistered or uninsured;

- (b) In violation of the inspection requirements set forth in section [insert citation to state vehicle inspection law];
 - (c) Registered to an individual for whom there is an outstanding felony warrant;
 - (d) Associated with a missing person;
 - (e) Stolen; or
 - (f) Related to or involved in a felony.
- (2) By parking enforcement entities for regulating the use of parking facilities;
 - (3) For the purpose of controlling access to secured areas; or
 - (4) For the purpose of electronic toll collection.
- (C) For the allowed uses under Section 2(B)(1)(a) and (b), it shall be unlawful to intentionally target enforcement towards a population based on race, ethnicity, or income level in a manner that exceeds that group's proportion of the overall population within the enforcing government entity's jurisdiction;
- (D) It shall be unlawful to operate or utilize any ALPR system whose operation is not fully compliant with the provisions of this Act.

Section 3. Protections.

- (A) Captured plate data collected by or on behalf of a government entity, as authorized pursuant to Section 2(B), shall not be used, shared, or accessed for any other purpose and shall be deleted after 48 hours, except that such data may be retained:
- (1) For as long as such captured plate data is needed as evidence of specific unlawful conduct enumerated in Section 2(B)(1);
 - (2) For as long as such captured plate data is needed to support the assessment and collection of a toll pursuant to Section 2(B)(4);
 - (3) Pursuant to a Section 4(A) preservation request;
 - (4) Pursuant to a disclosure order sought pursuant to Section 4(B); or
 - (5) Pursuant to a valid, court issued, probable cause warrant or other valid court order.
- (B) Notwithstanding the provisions of Section 3(A), captured plate data collected by or on behalf of a government entity, as authorized pursuant to Section 2(B), may only be used, shared, or accessed by an out-of-state person or entity pursuant to a valid, court issued, probable cause warrant or other valid court order.
- (C) Any government entity that uses an automatic license plate reader system pursuant to Section 2(B)(1) must update those systems from the databases

enumerated in Section 2(B)(1) in real-time, at the beginning of each shift, or whenever such updates are available.

Section 4. Preservation and Access.

(A) Preservation request.

(1) A government entity that operates or uses an automatic license plate reader system, upon the written request of a government entity or a defendant in a criminal case, shall take all necessary steps to preserve specified captured plate data in its possession pending the issuance of a court order sought pursuant to Section 4(B), if:

- (a) The requesting government entity or defendant in a criminal case requests such retention and specifies in a written, sworn statement:
 - (i) The particular camera or cameras for which captured plate data must be preserved or the particular license plate for which captured plate data must be preserved;
 - (ii) The date or dates and timeframes for which captured plate data must be preserved; and
 - (iii) That a court order for the retention and disclosure of captured plate data will be sought, pursuant to Section 4(B), in a court of competent jurisdiction within seven days of the transmission of the preservation request.

(B) A government entity or defendant in a criminal case may apply for a court order for the extended retention and disclosure of captured plate data, which shall be issued by any court of competent jurisdiction if the government entity or defendant in a criminal case offers specific and articulable facts showing there is probable cause to believe the captured plate data is relevant and material to an ongoing felony criminal or missing persons investigation, prosecution, or defense.

(C) Captured plate data retained by a government entity for more than 48 hours pursuant to a Section 4(A) preservation request shall be immediately destroyed if:

- (1) An application for a court order, pursuant to Section 4(B), is not made within seven days of the preservation request, or
- (2) The application for the court order, made pursuant to Section 4(B), is denied.

(D) Notice of a data deletion-triggering event, as enumerated in Section 4(C)(1) or (2), shall be provided within 24 hours of its occurrence by the person or entity who made the Section 4(A) preservation request to the recipient of that request.

- (E) A government entity may purchase, obtain, receive, or use privately captured plate data only pursuant to a valid, court issued, probable cause warrant.

Section 5. Data Sharing and ALPR access.

- (A) Any government entity that uses automatic license plate reader systems pursuant to Section 2(B) shall:
- (1) Not share or otherwise provide access to collected ALPR data unless the requesting party:
 - (a) Is a government entity that agrees not to further share the data unless otherwise required by law; or
 - (b) Has a judicially issued, probable cause warrant for the specific data.
 - (2) Not provide any other entity with direct access to the ALPR system.

Section 6. Reporting.

- (B) Any government entity that uses automatic license plate reader systems pursuant to Section 2(B) shall:
- (1) Consistent with the provisions of this Act, adopt a policy governing use of the system, prohibiting non-essential data collection and sharing, and protecting the security of data that is collected, the entirety of which shall be conspicuously posted on the government entity's Internet website;
 - (2) Report annually on its automatic license plate reader practices and usage to the state or local legislature that governs the government entity. The report must also be conspicuously posted on the government entity's Internet website. The report shall include:
 - (a) The number of license plates scanned;
 - (b) The names of the hot lists against which captured plate data were checked, and the number of matches generated by each hot list;
 - (c) The number of matches, by hot list, that resulted in arrest and prosecution;
 - (d) The number of preservation requests received under Section 4(A);
 - (e) The number of preservation requests issued under Section 4(A), broken down by the number of preservation requests issued to other government entities and the number of preservation requested issued to private automatic license plate reader systems;
 - (f) The number of disclosure orders received under Section 4(B);

- (g) The number of times ALPR data was shared with or accessed by another government entity;
- (h) The number of times ALPR data was shared or accessed pursuant to a judicial warrant; and
- (i) Any changes in policy that affect privacy concerns.

Section 7. No captured plate data and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the State of [insert state name], or a political subdivision thereof, if the collection or disclosure of that information was or would be in violation of this Act, unless such evidence is exculpatory in a criminal trial or proceeding.

Section 8. Penalties.

- (A) Any person who violates the provisions of this Act shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this Act has injured his business, his person, or his reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him on account of violation of the provisions of this Act, or liquidated damages of one thousand dollars, and a reasonable attorney's fee and other costs of litigation.

Section 9. Privacy.

- (A) Captured plate data shall not be considered a public record for the purposes of [insert citation to state open records law].
- (B) Notwithstanding Section 9(A), the following information shall be considered a public record for the purposes of [insert citation to state open records law]:
 - (1) An ALPR system's audit, use, and access logs and data; however, in responding to a valid request, any individual license plate information or other vehicle-specific identifying information, such as vehicle photographs and information regarding a vehicle's make, model, or color, shall be redacted from the responsive documents and data; and
 - (2) Data and information regarding a vehicle personally owned or leased by the [name of open records law] requestor during the period of ownership or lease; however, a request for such information shall only be permitted where, as part of the request:
 - (a) The requestor affirms, through a notarized, sworn statement, that the requester is the sole owner/lessor of the vehicle, and that no one other than the requestor drives the vehicle more than 10% of its total trips; or
 - (b) Where the requester is not the sole owner/lessor of the vehicle, or one or more other persons drives the vehicle more than 10% of

February 2026 Version

its total trips, the primary requestor, through a notarized, sworn statement:

- (i) Identifies every owner/lessor of the vehicle and every driver of the vehicle who drives the vehicle more than 10% of its trips;
 - (ii) Affirms that neither the primary requestor nor any other identified owner(s)/lessor(s) of the vehicle or other identified driver(s) is subject to an outstanding order of protection involving the primary requestor or any other identified owner(s), lessor(s), or identified driver(s) of the vehicle; and
 - (iii) Every owner, lessor, and driver identified pursuant to Section 9(B)(2)(b)(i) signs the request, thereby joining the primary requestor as a co-requestor in making the request.
- (c) For purposes of Section 9(B)(2), the terms “requestor”, “co-requestor”, “owner”, “lessor”, and “driver” shall only refer to human persons, and not any business, corporate, or other non-human entities.

Section 10. Severability.

The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person, entity, or circumstance, is held invalid, the remainder of this Act, including the application of such part or provision to other persons, entities, or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 11. Effective Date.

This Act shall take effect upon passage.

(Page intentionally blank)