CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: HONORABLE MAYOR AND CITY COUNCIL

FROM: Paul Joseph

SUBJECT: **See Below**

DATE: February 9, 2026

Approved

Date: 2/25/2026

COUNCIL DISTRICT: Citywide

SUBJECT: Automated License Plate Readers Data Usage Protocol Update

RECOMMENDATION

(a) Approve the following changes to the Police Department Automated License Plate Reader Data Usage Protocol:
   (1) Change the default retention period of data collected by the Automated License Plate Reader from "one year" to "30 days."
   (2) Prohibit placing Automated License Plate Reader cameras in positions that capture data from vehicles entering or exiting any reproductive health care services facility primarily providing abortion services or any location primarily used for religious observance.
   (3) Make other technical, non-substantive, or formatting changes.

(b) Accept the report on the Police Department's Automated License Plate Reader program and approve the following changes to the Automated License Plate Reader policy:
   (1) Require additional compliance documentation from California agencies requesting access to the Police Department's Automated License Plate Reader data, including the reason justification, the crime type, and a case number.
   (2) Require approval from a command staff officer before assisting agencies without existing access.
   (3) Require multi-factor authentication for all access to the Automated License Plate Reader system.

(c) Add the following clarification to the Police Department's public Automated License Plate Reader Transparency Portal:[1] "The San José Police Department only shares data with California law enforcement agencies subject to the

[1] https://transparency.flocksafety.com/san-jose-ca-pd

California Values Act (Senate Bill 54, 2017)[2] and Automated License Plate Recognition Systems: Use of Data (Senate Bill 34, 2015).[3] These laws prohibit information sharing with federal immigration enforcement. Transmittal of Police Department Automated License Plate Reader data to federal agencies for immigration enforcement is illegal."

SUMMARY AND OUTCOME

The recommended changes significantly tighten data security and access around the Police Department's Automated License Plate Reader (ALPR) program. Reducing retention to 30 days limits unnecessary historical storage consistent with common industry practices while still providing detectives with the data necessary to solve serious crimes. Restricting the placement of Automated License Plate Reader cameras reduces the risk of collecting data associated with sensitive locations. Requiring crime type, case numbers, and multi-factor authentication ensures appropriate documentation for access and usage. Public clarification reinforces compliance and trust, particularly around immigration protections.

BACKGROUND

San José's ALPR camera program is administered by the Police Department's (Department) Real Time Intelligence Center (RTIC). The ALPR program was implemented in May 2022, when four cameras were installed at the intersection of Curtner Avenue and Monterey Road pursuant to City Council direction. The initial deployment responded to multiple vehicular hit-and-run fatal collisions involving pedestrians at that location. In December 2022, additional ALPR systems with gunshot detection capability were installed in seven neighborhoods impacted by violent crime. As of today, 474 ALPR cameras are installed throughout San José.

In August 2022, City Council approved the Data Usage Protocol (DUP) for ALPRs, superseding the Department's prior DUP contained in Police Duty Manual section L 4207 – USE OF AUTOMATED LICENSE PLATE READER (ALPR) TECHNOLOGY. The DUP was developed in collaboration with the Information Technology Department, the City's Digital Privacy Officer, and the City Attorney's Office to ensure compliance with the City's Digital Privacy Policy (City Council Policy 0-46). It authorized the use of ALPR technology in compliance with state and local laws, established annual reporting requirements, and provided an ongoing mechanism for public feedback. Adoption of the DUP satisfied the requirements of California Civil Code section 1798.90.53,[4] which requires agencies to maintain a usage and privacy policy governing ALPR systems.

---

[2] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB54
[3] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB34
[4] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.90.53

California Civil Code section 1798.90.53 requires that ALPR usage and privacy policy specify, among other elements, the length of time ALPR data is retained. The August 2022 DUP established a default retention period of one year for ALPR data, while allowing data associated with criminal investigations to be retained for longer periods, in accordance with applicable state and federal evidentiary laws.

The August 2022 DUP also established prohibited uses of ALPR technology. These include collecting data not visible from a public place, monitoring constitutionally protected activity, sharing data for immigration enforcement purposes, engaging in automated enforcement without manual review by Department personnel, and selling ALPR data to any entity.

The Department maintains a public ALPR Transparency Dashboard on the Flock Safety website. The dashboard provides information regarding the ALPR program, including system capabilities and limitations, acceptable and prohibited uses, the number of cameras deployed, data retention practices, and the list of agencies authorized to access San José ALPR data.

In addition, the Department submits an annual ALPR data usage report to the City's Digital Privacy Officer. These reports include location-based metrics on license plates captured, alert activity, system access and queries, audit narratives, and any implemented or proposed program changes.

Recent reviews of the ALPR program identified opportunities to amend the DUP to address recent community concerns surrounding the use of this technology, and to further align the DUP with the City's Digital Privacy Policy, particularly with respect to data minimization and retention. A proposed draft of the revised DUP is attached to this memorandum. See Attachment: Data Usage Protocol for Automated License Plate Reader Technology Updated as of February 9, 2026.

ANALYSIS

The Department's ALPR program has expanded steadily since its implementation in 2022 and is now fully integrated into the RTIC. ALPR data is routinely incorporated into real-time and follow-up analysis and is used as an investigative resource across multiple Department elements, including Patrol, the Crime Analysis Unit, the Bureau of Investigations, Special Operations, and the Air Support Unit. As deployment and familiarity with the technology have increased, ALPR has become a regularly used tool to support time-sensitive investigations and broader case development.

During the first half of Fiscal Year 2025-2026, RTIC documented 56 notable cases in which ALPR data contributed to investigative outcomes. These cases included investigations involving violent crime, firearms-related offenses, child abductions, domestic violence incidents, robberies, felony hit-and-run collisions, burglaries, carjackings, and attempted kidnappings. These figures reflect only RTIC-documented

cases and do not capture ALPR usage occurring independently within other operational units.

Additional operational data further illustrates ALPR's role in supporting enforcement and investigative activity. Between January and October 2025, the Air Support Unit reported participating in 60 cases in which ALPR data was used, resulting in 73 arrests, 38 arrest warrants, and the recovery of more than $1 million in stolen vehicle value. These outcomes reflect ALPR's utility in supporting coordinated air and ground operations, particularly in vehicle-related crimes and suspect apprehension.

The Crime Analysis Unit reviews of reported incidents and calls for service referencing "ALPR" in the event details indicate a consistent pattern of increased use following camera placement, along with generally higher rates of cases cleared through arrest or citation during those periods. While ALPR is not determinative in every case and does not replace traditional investigative methods, the data shows that ALPR is most effective as a complementary tool, particularly for vehicle-related crimes, crimes against persons, and selected property offenses. Analysts observed that increases in ALPR usage were more strongly associated with cases resulting in criminal charges than with cases closed without enforcement action, suggesting a positive contribution to case solvability.

More broadly, Department workload trends provide additional context for ALPR's role within investigative operations. According to the Fiscal Year 2024-2025 Annual Services Report,[5] the Department assigned approximately 32,000 of the 53,400 cases it received for investigation. While this increase cannot be attributed to any single factor, the proportion of cases assigned for investigative follow-up has risen steadily in recent years, reflecting the integration of tools such as ALPR that support earlier identification of investigative leads and the generation of leads that would not have otherwise existed.

Collectively, these indicators demonstrate that ALPR has become an established and routinely utilized investigative resource within the Department. Its primary value lies in enhancing situational awareness, accelerating suspect identification, and supporting coordinated investigative and enforcement efforts across units, rather than serving as a standalone or independently operating technology.

With the demonstrated value of the program in mind, Department leadership and program managers have a responsibility to periodically review related policies to confirm consistency with the City's Digital Privacy Policy. That policy emphasizes data minimization, transparency, accountability, and appropriate safeguards for sensitive information. Several years of operational experience and familiarity with the technology have created an opportunity to refine the DUP while preserving the public safety benefits of ALPR use.

[5] https://www.sanjoseca.gov/home/showpublisheddocument/127267/639050165360500000

Reduction of ALPR Data Retention Period

Review of ALPR usage indicates that the existing one-year default retention period exceeds what is necessary for most investigative purposes. RTIC evaluated historical use cases and determined that reducing the default retention period to 30 days would have minimal impact on investigative effectiveness or operational support. ALPR data associated with active criminal investigations would continue to be retained in accordance with applicable state and federal evidentiary requirements. Reducing routine retention limits the amount of data stored without an investigative purpose and aligns with the City's data minimization principles. This change also results in an estimated annual reduction of approximately $142,200 in data storage costs, as described in the Cost Summary and Implications section.

Restrictions on ALPR Camera Placement at Sensitive Locations

The existing DUP already prohibits the use of ALPR technology to monitor activities protected by state law or the First Amendment. The proposed amendment provides additional clarity by addressing camera placement at certain sensitive locations. Under the amended DUP, ALPR cameras may not be positioned to capture vehicles entering or exiting any reproductive health care services facility primarily providing abortion services, such as Planned Parenthood, or locations primarily used for religious observance, such as churches, mosques, or temples.

The Department has reviewed current ALPR camera placement and confirmed that no existing cameras are configured to collect data from these locations. This amendment is intended to guide future deployment or relocation decisions and to establish clear constraints for program expansion. The clarification reinforces constitutional protections and reduces the risk of collecting data associated with lawful, protected activity.

Additional Documentation for External Agency Access

Sharing ALPR data with California law enforcement agencies remains an important investigative tool, particularly when criminal activity crosses jurisdictional boundaries. At the same time, the Department must maintain accountability and oversight for how ALPR data is accessed and used. Requiring requesting agencies to provide a crime type and case number, in addition to a justification for access, strengthens compliance review and auditability. This requirement ensures access requests are tied to a defined investigative purpose and supports responsible data-sharing practices.

Command-Level Approval for Agencies without Existing Access

Assisting other agencies that do not have existing access to the Department's ALPR system can support significant investigative efforts, particularly in complex or multi-jurisdictional cases. However, such assistance carries additional legal and policy considerations under California law. To ensure compliance and appropriate oversight, any San José employee requested to conduct an ALPR search on behalf of an agency without existing direct access shall obtain prior approval from a Department Commander before utilizing the system.

The approving Commander shall confirm that the requested search aligns with Department policy, applicable state law, and a legitimate law enforcement purpose. This approval requirement reinforces supervisory accountability and ensures that ALPR use remains consistent with California's statutory limitations on data access and sharing. Documentation of the Commander's approval shall be clearly recorded in the ALPR system's justification field, including the approving Commander's name and the date of authorization, to support auditability and post-use review.

Implementation of Multi-Factor Authentication

ALPR systems contain sensitive location-based data that requires appropriate security controls. Requiring multi-factor authentication for all ALPR system access reduces the risk of unauthorized use and strengthens system security. This change aligns with accepted data protection practices and does not affect authorized operational access.

Data Sharing and Immigration Enforcement

The Department has added clarifying language to its public ALPR Transparency Portal to describe legal limitations on data sharing. The clarification references the California Values Act (Senate Bill 54, 2017) and Automated License Plate Recognition Systems: Use of Data (Senate Bill 34, 2015), and states:

> *The San José Police Department only shares data with California law enforcement agencies subject to the California Values Act (Senate Bill 54, 2017) and Automated License Plate Recognition Systems: Use of Data (Senate Bill 34, 2015). These laws prohibit information sharing with federal immigration enforcement. Transmittal of San José Police Department ALPR data to federal agencies for immigration enforcement is illegal.*

Including this language on the public-facing dashboard improves transparency, reinforces compliance with state law, and provides clear information to the community regarding how ALPR data may and may not be used.
The Department utilizes additional safeguards available within the Flock ALPR platform to further limit data sharing and search functionality. The platform allows the Department to disable "Federal Sharing" by toggling off the ability to receive sharing

requests from federal organizations. The Department has disabled Federal Sharing and has chosen not to receive sharing requests from federal organizations.

The Flock platform also provides configurable search filters. As described on the Flock website, "*These filters are designed to remove your organization's devices from any search that appears to indicate that the search is connected to either immigration enforcement or reproductive care. The filter will apply to all searches performed that would include any of your networks, whether by users in your organization or other agencies you share with, such as via direct one-to-one sharing and the Statewide and Nationwide Lookup tools (if applicable).*" The Department has enabled both the "Filter out Immigration searches" and "Filter out Reproductive Care searches" settings. These safeguards provide an additional technological layer of protection beyond statutory and policy restrictions.

On February 4, 2026, the Department conducted an internal search history audit of the Flock Automated License Plate Reader system (organization audit) for calendar year 2025. The review confirmed that all Department use justifications were in compliance with Department policy and California law. Additionally, the Department conducted an external agency search history audit of the Flock ALPR system for calendar year 2025. The audit identified several external searches with limited justification information. RTIC staff personally contacted each agency for additional clarification and confirmed that all searches were in compliance with Department policy and California law.

The Department will conduct quarterly internal and external audits to ensure continued compliance with Department policy and applicable state law.

Collectively, these changes strengthen privacy protections, improve accountability and data security, and align Department practices with City policy and state law, while preserving the operational value of ALPR technology in support of public safety.

EVALUATION AND FOLLOW-UP

Implementation and ongoing compliance with the revised ALPR DUP will be monitored by the RTIC Commander. Program effectiveness, adherence to policy requirements, and any identified compliance issues will continue to be reviewed through established oversight processes. Findings, conclusions, and any recommended adjustments will be documented and reported through the Annual Data Usage Report for ALPRs.

COST SUMMARY/IMPLICATIONS

Reducing the default retention period for ALPR data from one year to 30 days will result in a reduction in annual data storage costs. The ALPR data storage subscription model is priced $300 lower per camera per year for a 30-day retention period compared to the one-year retention plan, for a total annualized savings of approximately $147,000.

The City currently deploys 490 cameras, of which 190 are funded in the General Fund at an annual ongoing cost of $580,000, and 300 are funded by the 2023-2024 Board of State and Community Corrections Organized Retail Theft Grant at an annual amount of approximately $900,000. However, this grant expires in December 2026; the continuation of the cameras currently funded by the grant will be evaluated as part of the 2026-2027 Proposed Budget development process in context of the General Fund's budgetary position and other critical City Council priorities.

The savings attributed to the 190 cameras currently funded ongoing in the General Fund is approximately $57,000 and will be incorporated in the Police Department's 2026-2027 Base Budget.

The other proposed updates to the ALPR DUP are policy and security related and are not expected to result in any new additional costs.

COORDINATION

This memorandum has been coordinated with the City Attorney's Office, the City Manager's Budget Office, and the Information Technology Department.

PUBLIC OUTREACH

This memorandum will be posted on the City Council Agenda website for the March 10, 2026 City Council meeting.

COMMISSION RECOMMENDATION AND INPUT

No commission recommendation or input is associated with this action.

CEQA

Not a Project, File No. PP17-008, General Procedure and Policy making resulting in no changes to the physical environment.

PUBLIC SUBSIDY REPORTING

This item does not include a public subsidy as defined in section 53083 or 53083.1 of the California Government Code or the City's Open Government Resolution.

Police Chief
Police Department

The principal author of this memorandum is Lieutenant Nathaniel Bennett, San José Police Department Research and Development Unit. For questions, please contact nathaniel.bennett@sanjoseca.gov or the Research and Development Unit at (408) 277-5200.

ATTACHMENT:

Data Usage Protocol for Automated License Plate Reader Technology Updated as of February 9, 2026

City of San José
Data Usage Protocol (DUP) for Automated License Plate Reader (ALPR) Technology

Owning department(s): San José Police Department (SJPD)
Department owner: Deputy Chief, Executive Officer

1) Purpose

Automated License Plate Readers (ALPRs) use high speed cameras to photograph vehicle license plates. The purpose of ALPR cameras is to improve criminal investigations[6] and deter crime in the surrounding area.[7] This Data Usage Protocol (DUP) defines for the City of San José's (hereafter referred to as "City") Police Department ("hereafter referred to as "Department"):

1. Authorized usage of ALPR technology that complies with State and local laws;
2. Annual reporting requirements on ALPR usage; and
3. An ongoing avenue for public feedback on ALPR usage.

This DUP is also meant to ensure that San Jose Police Department's use of Automated License Plate Recognition (ALPR) technology complies with all applicable federal, state, and local laws. For the purposes of California law, this document serves as the "usage and privacy policy" as required by California Civil Code Sections 1798.90.53

2) Authorized Uses:

The Department shall use ALPR technology with the goal of reducing serious crime and traffic incidents in the long term. ALPR is meant to act as a deterrent for crime and dangerous driving in a neighborhood, and to support police in criminal investigations. ALPR vendors may only use the data if authorized by the City to act on behalf of the City. The Department and authorized vendors may utilize ALPR technology and any data generated only to do the following:

1. Use in conjunction with any patrol or investigative function in response to the investigation of felony or misdemeanor crimes;
2. Locate at-risk missing persons (including responding to Amber and Silver Alerts);
3. Support local and State safety departments in the identification of vehicles associated with criminal investigations. Further detail on permissible sharing and coordination with safety departments is detailed in the "Data Sharing" section below; and

[6] Koper, Christopher S., and Cynthia Lum. "The impacts of large-scale license plate reader deployment on criminal investigations." Police Quarterly 22.3 (2019): 305-329 – https://journals.sagepub.com/doi/abs/10.1177/1098611119828039

[7] Koper, Christopher S., Bruce G. Taylor, and Daniel J. Woods. "A randomized test of initial and residual deterrence from directed patrols and use of license plate readers at crime hot spots." Journal of Experimental Criminology 9.2 (2013): 213-244 – https://link.springer.com/article/10.1007/s11292-012-9170-z

4. Automatically initiate investigation for traffic intersection infractions through a device (e.g., red-light violations) if SJPD follows the requirements outlined in California Vehicle Code 21455.5,[8] including providing notice of automated enforcement within 200 feet of the intersection.

3) Prohibited Uses:

ALPR technology will not be used for the following purposes:

1. Collect data that is not within the public view. This includes any data not readily visible from a public area or public property;
2. Monitor individual or group activities legally allowed in the State of California and/or protected by the First Amendment to the United States Constitution;
3. Share with immigration authorities or use in the investigation of any matter related to immigration status of an individual;
4. Engage in automated citations or other automated enforcement without manual review from SJPD staff; and
5. Sell any data generated by ALPR to any entity.

ALPR cameras will not be placed in positions that capture data from vehicles entering or exiting any reproductive health care services facility primarily providing abortion services or any location primarily used for religious observance.

4) Operational Procedures

The ALPR system(s) and their associated database(s) shall only be used for official law enforcement purposes listed in the "Authorized Uses" section. Additionally:

1. No member of the Department shall operate, utilize and/or search ALPR systems and their associated equipment/database(s) without first completing Department-approved training and only if the operation, utilization, or searching complies with SJPD's need to know/right to know protocols defined in SJPD Duty Manual section C2000 on criminal records and information;[9]
2. Once an alert is received, the officer will make every effort to visually confirm that the captured license plate from the ALPR system matches the license plate of the observed vehicle;
3. In all instances, before any action is taken based solely upon an ALPR alert, the officer will make every effort to verify the alert is still valid through the California Law Enforcement Telecommunications System (CLETS). Officers will not take any action that restricts the freedom of any individual based solely upon an ALPR alert until an attempt at verification has been made;
4. If the reason for an ALPR alert pertains to a wanted person associated with a vehicle, officers should attempt to visually inspect the occupant(s) of the

[8] California Vehicle Code "Offenses Relating to Traffic Devices" - https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=21455.5.&nodeTreePath=15.2.3&lawCode=VEH

[9] See SJPD Duty Manual - http://www.sjpd.org/records/dutymanual.asp

vehicle to determine if he/she matches the description of the wanted individual. Absent this verification, officers must have a separate legal justification to conduct a vehicle stop;

5. Designation of vehicles into "hot lists"[10] shall be the sole responsibility of the assigned investigating officer or his/her designee. Vehicles cannot be entered into "hot lists" without a lieutenant's approval. It will be the arresting/investigating officer's responsibility to ensure timely entry/removal of license plates into/out of the designated "hot lists".
6. To the best of the system administrator or his/her designee's ability, hot lists managed by an external source (e.g., the Stolen Vehicle System) will be synchronized with the external hot list at all times. In the event of a loss of connection to external hot lists, the ALPR system administrator or his/her designee shall synchronize with external hot-lists upon reconnection;
7. Protocols shall be established to ensure timely notification is made to the system administrator to indicate and record when a "hot list" ALPR license plate capture is made and the ultimate disposition of the specific enforcement action;[11] and
8. All vehicles entered into a departmental "hot list" will contain the following information:
    a. Name, badge number and assignment of department member entering the information (e.g., Officer Smith #1234, Robbery Unit)
    b. Associated case number(s)
    c. Short synopsis describing the reason for the vehicle/occupant database entry. This should include the presumed crime or crimes relevant to this investigation. If no crime is relevant, state the other purpose (e.g., Amber alert)

5) Data Collection

ALPR utilizes high speed cameras angled to capture digital images of vehicle license plates on public roads and private property visible from a public road (e.g., a driveway). The cameras are trained on the license plate of a vehicle and rarely capture the image of a person. The cameras do not identify an individual or group based on physical characteristics such as skin-tone, body shape, or facial features.

An example image captured from an ALPR camera is provided in Figure 1. While the ALPR camera is angled to capture license plate information, it may collect additional information visible in the image, including car make/model, and other distinguishing characteristics of the vehicle (e.g., bumper sticker(s), aftermarket wheels, etc.).

ALPR cameras may be placed in a fixed location, such as on a street light pole, or in

[10] License plate(s) associated with vehicles of interest from an associated database, including, but not limited to: California Law Enforcement Telecommunications System (CLETS), National Crime Information Center (NCIC), Be on the Lookout notices (BOLOs), and Department databases

[11] An example notification would be: "Hot list 211A vehicle alerted at Curtner/Monterey, observed at Curtner/Malone. Vehicle stopped, driver arrested for 211"

a roaming location, such as on a police vehicle. The technology will record the date and time the image was captured as well as the location of the camera. The exact location of a vehicle is not tracked but can be inferred based on the location of the camera at the time of the photograph.

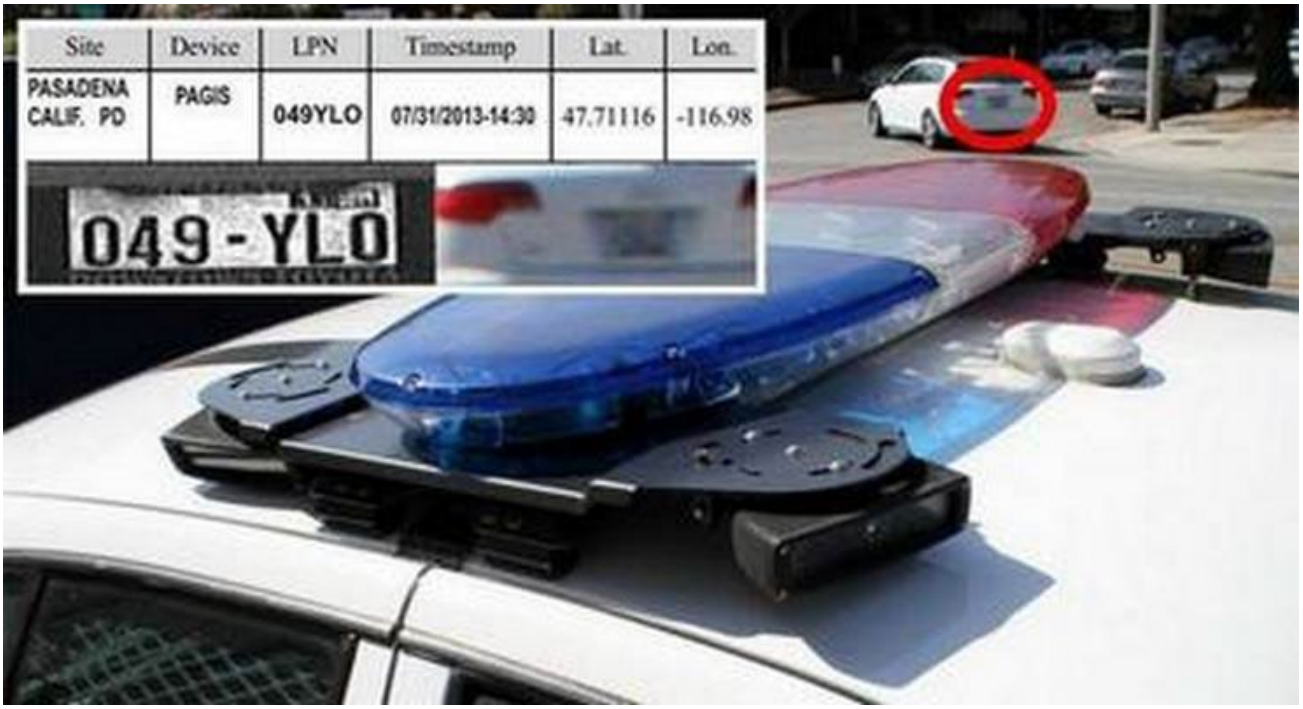

Figure 1: Police vehicle with an Automated License Plate Reader mounted on its roof, and an example picture from the ALPR camera (top-left). This ALPR picture identifies 1) the license plate, 2) the time and location of the car, and 3) other information captured in the photograph, including vehicle color, make, and model. Source: Pasadena, CA Police Department. https://www.pasadenanow.com/main/city-council-to-consider-purchasing-more-automatic-license-plate-readers

6) Notice

Notice that the City of San José is using ALPR technology will be posted as signage at major vehicle entrances into the city and exits from the city, and at "designated intersections" within the city to notify residents that ALPR cameras may be present in their area.

"Designated intersections" refers to locations near where ALPR technology is being utilized. The signs will contain notice that ALPR technology is in use and will direct the reader to where they can get more information about the ALPR program and policies. Notice and additional detail, including this Data Usage Protocol, will be available on the City website.

7) Retention and Minimization

Data collected from ALPR technology will be retained for thirty (30) days. Once the

retention period has expired, the record shall be purged entirely from all active and backup systems unless the data is related to an active investigation of a crime not listed in the “Prohibited Uses” section.

Data associated with a criminal investigation may be stored for longer on an electronic storage device or printed and retained in accordance with applicable state and federal evidentiary laws, to include retaining the data through the adjudication of a case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations.

8) Access and Accuracy

Raw ALPR data, including photographs, license plates, location, and associated hot list data will not be available for public access unless required pursuant to city, state, or federal law, or a court order. Aggregated data on the ALPR technology, including performance metrics on the accuracy of the technology, will be made available annually in the Annual Data Usage Report. More details on the Annual Data Usage Report can be found in the “Annual Data Usage Report requirements” section below. The City may release more aggregated data periodically at its discretion.

9) Accountability

All Department members authorized to use or access ALPR technology or data shall be accountable for knowledge of this protocol. See “Training” section for definition of authorized personnel.

All access to the system shall be logged, and the Department will maintain an audit trail of requested and accessed information, including the purpose of the query. Periodic, random audits shall be conducted by a unit other than the Real Time Intelligence Center (RTIC) at the direction of the Deputy Chief, Executive Officer to ensure and evaluate compliance with system requirements and with the provisions of this protocol and applicable law. Audit trails shall be maintained by the Department for a minimum of two (2) years. Additional audits or reviews may be triggered at the direction of the City Council or Digital Privacy Officer (DPO), consistent with state law and authorized access to information.

If a Department member accesses or provides access to ALPR information, the Department member shall do the following:

1. Maintain a record of the access that includes the following information:
    a. Date/Time the Information was accessed
    b. The license plate number or other data elements used to query the ALPR system
    c. The name and department of the person who accessed the information
    d. The purpose for accessing the information, including the presumed crime or crimes relevant to this investigation. If no crime is relevant, state the other purpose (e.g., Amber alert)
2. ALPR information may only be used for authorized purposes as specified in

this protocol in accordance with California Civil Code section 1798.90.51(b).

10) Sharing

The City does not share ALPR data with any contracted, commercial, or private entity. The provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR information (see CA Civil Code 1798.90.55.(b)).

Information gathered or collected, and records retained by the City will not be:

1. Sold, published, exchanged, or disclosed for commercial purposes;
2. Disclosed or published without authorization; or
3. Disseminated to persons not authorized to access or use the information.

The City shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law. The City may agree to share access to its ALPR database by law enforcement agencies within the State of California on an agency-by-agency basis if an agreement is put into place.

The data will not be shared beyond the approved agencies. All agencies must request SJPD ALPR data directly from SJPD (e.g., if SJPD shares ALPR data with Santa Clara PD, Sunnyvale PD must request SJPD data through SJPD rather than Santa Clara). The requesting agency may only access the data for an authorized purpose, as noted in this protocol.

Logs will be generated every time an approved law enforcement agency accesses data from SJPD's ALPR system, which will include:

a. Date/Time the Information was accessed
b. The license plate number or other data elements used to query the ALPR system
c. The name and law enforcement agency of the person who accessed the information
d. The purpose for accessing the information

11) Equity and Community Engagement

The City will make a reasonable effort to identify and mitigate any inequity inherent in the ALPR technology and its implementation. Members of the public may submit any concerns via the public comment feature at sanjoseca.gov/digitalprivacy. Comments may also be submitted by emailing digitalprivacy@sanjoseca.gov or mailing the Digital Privacy Officer at 200 E Santa Clara St. San Jose CA 95113, 11th Floor. ALPR implementations can impact certain populations more than others. The City of San Jose is cognizant of that concern and will field potential complaints when submitted by emailing: digitalprivacy@sanjoseca.gov. After receiving a complaint, the City will perform an investigation and determine a corrective action plan, if necessary.

12) Storage and Security

Data collected by ALPR technology shall be stored in a secured police facility or secured third-party hosting environment. With the exception of audits, access to the raw data (images of vehicles and license plates) shall be limited to law enforcement staff with a legitimate need and right to access the information. The Department will utilize reasonable physical, technological, administrative, procedural, and personnel security measures to prevent unauthorized access to ALPR data. Authorized sworn personnel or authorized civilian personnel (such as a crime analyst) shall have general user access to the SJPD ALPR database, as appropriate, to query information. See "Training" section for definition of "authorized personnel". Entities authorized to audit the ALPR system (see "Accountability" section for who can authorize) do not need to be a part of the Department to access the database. Sworn personnel or authorized civilian personnel as approved by the Deputy Chief, Executive Officer, or his/her designee shall have administrative user access to the SJPD ALPR database, as appropriate, to control:

1. The information to which a particular group or class of users can have access based on the group or class;
2. The information a class of users can access, and/or data being utilized in specific investigations;
3. Sharing capabilities with other law enforcement agencies; and
4. Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the data or equipment.

The Bureau of Technical Services Systems Development Unit may provide ALPR technical support for the RTIC. The RTIC shall ensure compliance with this protocol. The custodian of ALPR data for purposes of this protocol shall be the Deputy Chief, Executive Officer or his/her designee.

In the event of a confirmed data breach where personal information such as license plate numbers or photographs have been accessed by an unauthorized party, the Department will follow the City of San José's Incident Response Plan. This security protocol and further security details are overseen by the City's Cybersecurity Office.

13) Training

Except for audits, only authorized personnel, meaning Department personnel trained in the use of ALPR technology, including its privacy and civil liberties protections, shall be allowed access to ALPR data. Training shall consist of:

1. Legal authorities related to the use of ALPR data and technology;
2. Current Department Data Usage Protocol regarding authorized use of ALPR technology;
3. Technical, physical, administrative, and procedural measures to protect the security of ALPR data against unauthorized access or use; and
4. Practical exercises in the use of ALPR technology.

14) Annual Data Usage Report requirements

To provide the City and the public with ongoing reporting on the usage and accuracy of the ALPR technology, the following information will be required in an Annual Data Usage Report submitted every year to the Digital Privacy Officer (DPO) no later than March 1st and covers the previous calendar year (January 1st – December 31st). In the year this Data Usage Protocol goes into effect, the Department is only required to report on the period from the date the Data Usage Protocol goes into effect until the end of the calendar year.[12] The Digital Privacy Officer will release the report to the public once private, confidential, and otherwise sensitive information is removed. The DPO shall release the report within 90 days of receiving it from the department, unless additional time is required to remove private, confidential, and sensitive information. If the DPO needs additional time, they shall provide a notice of extension to the public via the Digital Privacy webpage.[13]

1. Summary of the project and updates since the prior year, including detail on value to the department
2. Plans for future years, including any planned expansion of project or shift in data usage
3. Reporting metrics on ALPR usage and accuracy including:
    a. **# of reads by location** – the Department will either:
        i. Report directly the number of reads by location; or
        ii. Provide the Digital Privacy Officer (DPO) with access to the ALPR reads database, including the latitude and longitude of each read, from which the DPO can report by location as needed.
    b. **# of hits by location** – Similar to the # of reads by location, the Department will either:
        i. Report directly the number of hits by location; or
        ii. Provide the DPO with access to the ALPR reads database, including the latitude and longitude of each read and if the read was a hit, from which the DPO can report by location as needed.
    c. **Records accessed by SJPD** – the Department will report on the number of records accessed in accordance with the Accountability section of this Protocol.

Accuracy of accessed records – the Department will report on the accuracy of the implemented ALPR technology as requested by Council and the DPO.

[12] If this Data Usage Protocol is passed after September 30th, the first Annual Data Usage Report will not be required until the following year, which will cover usage from the date the Data Usage Protocol goes into effect to December 31st of the following year

[13] Link to the digital privacy webpage: https://www.sanjoseca.gov/your-government/departments-offices/information-technology/digital-privacy