



Memorandum

TO: RULES AND OPEN
GOVERNMENT
COMMITTEE

FROM: Councilmember Kamei
Councilmember Tordillos
Councilmember Cohen
Councilmember Mulcahy

SUBJECT: AUTOMATED LICENSE
PLATE READER DATA
ACCESS AND
SAFEGUARDS

DATE: September 23, 2026

Approved:

Rosemary Kamei David Cohen Anthony Tordillos
Michael Mulcahy

RECOMMENDATION

1. Direct the City Attorney, in coordination with the City Manager, to develop and present to City Council a draft ordinance defining and prohibiting the unauthorized access, use, or disclosure of Automated License Plate Reader (ALPR) data, including potential civil and criminal penalties for violations thereof, and, to the extent legally permissible, authorizing a private right of action against individuals responsible for such violations for individuals harmed by the unauthorized disclosure or misuse of ALPR data, with appropriate safeguards and enforcement considerations.
2. Direct the City Manager to:
 - a. Prohibit access to ALPR systems and data through personal devices;
 - b. Restrict off-duty access to ALPR systems except for defined law enforcement purposes; and
 - c. Incorporate said prohibitions and restrictions into applicable City and Police Department policies and procedures.
3. Direct the City Manager to evaluate additional authentication, access control, and auditing safeguards for ALPR systems, including multi-factor authentication and

automated tools to identify potentially unauthorized access or use, and to return to City Council with implementation options, associated costs, and any facilitating policy changes.

4. Direct the City Manager, in coordination with the City Attorney, the Independent Police Auditor (IPA), Information Technology Department (ITD), and San Jose Police Department (SJPd) to explore developing a process that enables the IPA to act as an independent auditor for ALPR practices, within the scope of the IPA's role under the charter. The IPA, ITD, and SJPd should establish and return to City Council with the audit methodology, scope, frequency, and procedures, with appropriate safeguards.

BACKGROUND

Automated License Plate Reader (ALPR) technology utilizes cameras and software to capture license plate information for law enforcement purposes. The City of San José relies on ALPRs as part of its law enforcement strategy. The City has also recognized that ALPR technology requires safeguards to balance its public safety applications with personal liberty, privacy, security, and equity considerations. To that end, the City has established policies governing the San José Police Department's (SJPd) use of ALPRs. The City's Data Usage Protocol, for instance, establishes requirements for authorized use, retention, access, and sharing of ALPR data and is intended to ensure compliance with applicable laws and Council-set policies.

On March 10, 2026, City Council unanimously approved a series of updates to SJPd's ALPR Data Usage Protocol and related policies.¹ These changes reduced the default retention period for ALPR data from one year to 30 days; prohibited camera placement that captures vehicles entering or exiting certain sensitive locations, including reproductive health care facilities, places of religious observance, consulates and embassies, and facilities primarily providing gender-affirming care; strengthened requirements governing data access by other California law enforcement agencies; and required additional safeguards governing access and use of the system.

As part of that action, City Council also directed the City Manager to continue audits of the ALPR program through the Information Technology Department (ITD), with findings to be reported through the Public Safety, Finance and Strategic Support Committee; explore alternative ALPR vendors; prohibit integration with facial recognition and biometric analysis software; and examine whether ALPR data could be used to train generative artificial

¹ See <https://sanjose.legistar.com/View.ashx?M=F&ID=15279913&GUID=F5A3F78C-488C-4982-A9DC-EFFD550773B4>

intelligence models.² Importantly, City Council further directed that any unauthorized disclosure or leak of ALPR data be reported by SJPd to City Council through an Information Memorandum and called for a protocol responding to unauthorized or unlawful disclosure of ALPR data.³

These safeguards were considered and adopted amid continued community concern regarding the privacy and security implications of ALPR technology. Concerns about the misuse of ALPR data are not unique to San José. A 2026 Washington Post investigation identified at least 50 law enforcement officers nationwide who had been charged with or accused of misusing ALPR systems, including 26 cases involving the alleged monitoring of women.⁴ These cases demonstrate the potential for technology intended for legitimate law enforcement purposes to be abused for personal surveillance, stalking, or harassment, particularly when access controls and auditing mechanisms fail to identify unauthorized activity.

This month, SJPd announced the termination of an officer following an investigation into the officer's misuse of the City's ALPR system.⁵ According to SJPd and subsequent reporting, the officer accessed the ALPR system from a personal device while off duty and provided the location of a vehicle to a relative who was the suspect in a domestic violence case. The relative then used that information to locate the individual who had accused him of domestic violence. The investigation was initiated after the victim reported to SJPd that the suspect appeared to know her exact whereabouts, raising the question about whether existing auditing and monitoring systems would have independently identified the misuse.

City Council's March 2026 action established expectations regarding the protection, oversight, and disclosure of ALPR information. The incident that resulted in this month's termination raises serious questions about the adequacy of these expectations and about the information presented to Council when it developed them. As such, we should consider whether additional safeguards are needed to prevent inappropriate access or disclosure, strengthen independent oversight, and demonstrate to the community that violations involving sensitive information result in meaningful institutional action.

² Concerns regarding Flock Safety have arisen across Santa Clara County and neighboring jurisdictions following incidents involving unauthorized access to ALPR data. In Mountain View, unapproved law enforcement agencies conducted searches of the City's ALPR records despite City policy requiring individual agency approval. The Mountain View City Council subsequently unanimously voted to terminate its contract with Flock Safety in February 2026. That same month, the Santa Clara County Board of Supervisors ended the County's use of Flock as the ALPR vendor serving the cities of Saratoga, Cupertino, and Los Altos Hills while considering additional safeguards.

³ See <https://sanjose.legistar.com/View.ashx?M=M&ID=1345647&GUID=80B0B36E-0C51-4E3E-AFB6-763D3E59F283>

⁴ See <https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes/>

⁵ See <https://www.mercurynews.com/2026/09/11/san-jose-police-officer-fired-for-abusing-flock-license-plate-reader-database-chief-says/>

ANALYSIS

The recent misuse of ALPR data demonstrates that written restrictions alone fail to suffice when the City lacks adequate mechanisms to deter misuse, identify it when it occurs, and provide accountability when violations cause harm. San José's existing protocol requires ALPR access to be logged, and limits use to authorized purposes, yet the conduct described above only came to light following a report from the victim.⁶ The recommendations in this memorandum are intended to strengthen the safeguards surrounding a technology that can reveal highly sensitive information about an individual's movements and location.

The City should ensure that intentional misuses of this information carry clear and enforceable consequences. Directing the City Attorney to develop an ordinance defining and addressing unauthorized access, use, and disclosure would provide an opportunity to establish appropriate civil and criminal penalties and evaluate a private right of action for individuals whose safety is threatened by the misuse of ALPR data.

The circumstances also demonstrate the importance of deterring misuse proactively. Enhanced authentication requirements, auditing tools, and other access controls could help flag potentially unauthorized searches before harm is caused. Previous Council direction should also be implemented and interpreted broadly enough to encompass all forms of unauthorized misuse of ALPR data, rather than applying only to an external data breach, leak, or disclosures to another entity or jurisdiction. The circumstances described in this memorandum demonstrate that improper use by an individual with otherwise authorized access can pose the same, or potentially greater, risks to the community's privacy and safety.

Finally, independent oversight should be part of the City's approach to rebuilding and maintaining public trust. Providing the Independent Police Auditor appropriate access to ALPR records for independent auditing would create additional mechanism to evaluate compliance and ensure safeguards are functioning as intended. Together, these measures would strengthen prevention, detection, accountability, and independent oversight of ALPR use in San José.

⁶ The term "authorized" may be overly broad where an individual has legitimate credentials to access the ALPR system but uses that access for an improper purpose. This distinction highlights the need to more clearly define what constitutes authorized and unauthorized access and use of ALPR data as outlined in the Recommendation.

RULES AND OPEN GOVERNMENT COMMITTEE

September 30th, 2026

Subject: Automated License Plate Readers Access and Safeguards

Page 5

The signers of this memorandum have not had, and will not have, any private conversation with any other member of the City Council, or that member's staff, concerning any action discussed in the memorandum, and that each signer's staff members have not had, and have been instructed not to have, any such conversation with any other member of the City Council or that member's staff.