Is Our Flock of ALPR Cameras Properly Tended?

San Mateo County Civil Grand Jury
2025-2026

Release Date: August 3, 2026

ISSUE

Over the past year, Automated License Plate Readers (ALPRs) have come under increasing public scrutiny. This report examines whether ALPR operators in San Mateo County (SMC) are in full compliance with applicable California law and whether their practices align with their adopted ALPR policies.

SUMMARY

Automated License Plate Readers have become widely deployed in SMC, with more than 500 cameras now in operation by law enforcement agencies (LEAs) within the County. The rapid increase in ALPR deployment has been accompanied by California legislation governing ALPR use, and also by increased media coverage of alleged violations. Over the past year, SMC LEAs have made notable operational improvements, particularly with respect to out-of-state data sharing. Most changes were driven by stronger default compliance made by Flock Safety (Flock), now the dominant ALPR platform among the SMC operators reviewed. But SMC ALPR operators continue to have many of the same operational deficiencies identified by a 2019 California State Audit that investigated four operators elsewhere in California. Many of the required policy documents are deficient or need significant revision to accurately reflect current operations, and audit materials produced were inconsistent in scope and rigor. Although the materials reviewed did not identify current sharing by SMC operators with out-of-state entities, most operators did not document criteria, process, or controls governing in-state sharing in a manner sufficient to demonstrate compliance with law. This report presents findings and recommendations to promote transparent operation of ALPR systems consistent with public safety, privacy, and applicable law.

BACKGROUND

Automated License Plate Readers

Automated License Plate Readers (ALPRs) are camera-based systems that automatically capture and analyze license plates on passing vehicles. Cameras are typically located at fixed roadside locations along high-traffic corridors, major intersections, city entry/exit routes, areas with high crime rates, and transportation infrastructure (bridges, tunnels, freeways). These systems combine high-speed cameras, infrared illumination, and optical character recognition software to convert license plate images into searchable digital data. Law enforcement agencies use ALPR systems to locate stolen vehicles, identify vehicles connected to criminal investigations, generate investigative leads, and assist in locating missing persons. When connected through regional or national networks, ALPR systems allow investigators to reconstruct vehicle movements across jurisdictions.

Digital imaging, optical character recognition, and large-scale data storage allow ALPR systems to process large numbers of license plates quickly and automatically. Modern systems can read thousands of plates per hour and store the results in databases that investigators can search later.

When a motor vehicle is detected by an ALPR as it passes through the camera's field of view, a digital record is generated recording the vehicle's license plate number, an image of the plate, a

contextual image of the vehicle (make, model, color, etc.), the date and time of the scan, the location of the camera, and the identification number of the camera device. Once the image is captured, the digital record is immediately transmitted to a cloud-based database that compares the scanned license plate and other vehicle data against law enforcement watch lists, often referred to as "hot lists," that may include information on vehicles that have been reported stolen, those associated with criminal investigations, outstanding warrants, or connected to missing persons or Amber Alerts. When a match occurs, the system can send an alert to officers or dispatch centers in real time.

ALPR cameras are usually deployed as part of a network such that when the same vehicle is detected by multiple cameras, investigators can analyze those detections to determine travel routes and timelines. By default, only data captured by cameras within that local jurisdiction are available. LEAs typically elect to contribute their data to regional databases or multi-jurisdictional systems that allow sharing across multiple cities, counties, or states. The ability to share data among multiple jurisdictions is more effective in assisting law enforcement in their investigations as suspects rarely limit their travel within a single jurisdiction.

As of March 30, 2026, more than 582 ALPR cameras were deployed across SMC. These cameras are operated by municipal police departments within their respective jurisdictions and by the San Mateo County Sheriff's Office (SMCSO) in unincorporated areas and in jurisdictions where the Sheriff provides contracted law enforcement services. The only police department in SMC with no ALPR cameras is Broadmoor.

Operator	Cameras as of 3/30/2026	Comments
Atherton	53	Earliest in SMC, 2020.
Belmont	10	
Brisbane	16	
Burlingame	18	
Colma	11	
Daly City	44	
East Palo Alto	25	
Foster City	20	
Half Moon Bay	14	Separate Flock contract, operated by SMCSO.
Hillsborough	22	
Menlo Park	32	
Pacifica	10	
Redwood City	25	
San Bruno	54	
San Mateo	66	

Operator	Cameras as of 3/30/2026	Comments
San Mateo County Sheriff's Office	109	Includes unincorporated SMC (except Broadmoor), Portola Valley, San Carlos and Millbrae.
South San Francisco	37	
Woodside	26	Separate Flock contract, operated by SMCSO

Key Issue

ALPRs and the sharing of image data across jurisdictional lines have created controversy with respect to issues of privacy. While not the focus of this report, some civil liberties groups, including the American Civil Liberties Union (ACLU), argue that vehicle tracking could affect freedom of association if it reveals attendance at protests, political meetings, or religious gatherings (First Amendment).

Others, including the Electronic Frontier Foundation (EFF) question whether large-scale tracking of vehicle locations over time could constitute a search under constitutional law (Fourth Amendment). While the focus of this report is not to investigate the constitutional issues surrounding ALPRs, data sharing among law enforcement agencies has become a significant public concern and has, in some communities, resulted in the suspension or termination of ALPR programs. Although no such actions have occurred in SMC, several Bay Area jurisdictions—including Mountain View, Los Altos Hills, Santa Clara County, and Santa Cruz—have discontinued their use of ALPR systems.

This report evaluates, based on records obtained during the investigation, whether SMC LEAs satisfy California law governing the use of ALPR systems and the sharing of ALPR data. Civil Code section 1798.90.51 requires APLR operators to implement and publicly post a usage and privacy policy. This report also evaluates whether the policies produced accurately describe actual operations.

Legislative Framework

California has enacted legislation governing the use of ALPR systems, with a focus on transparency, accountability, and limitations on data sharing. The primary statutory framework was enacted by Senate Bill 34 (SB 34) (Stats. 2015, Ch. 532), codified at Civil Code sections 1798.90.5 through 1798.90.55.

Effective January 1, 2016, SB 34 imposes requirements governing the collection, storage, access, and sharing of ALPR data. SB 34 applies to both operators of ALPR systems and entities that access ALPR data. Among other requirements, ALPR operators must adopt written usage policies, maintain detailed audit logs, implement reasonable security measures, and provide an opportunity for public comment prior to implementing an ALPR program. The California Department of Justice has issued guidance on SB 34 in Information Bulletin No. 2023-DLE-06.

In addition to SB 34, Senate Bill 54 (SB 54) (Stats. 2017, Ch. 495), known as the California Values Act (Gov. Code § 7284 et seq.) restricts the use of state and local law enforcement resources for

federal immigration enforcement purposes. SB 54 limits the sharing of certain information with federal immigration authorities and reinforces the principle that local law enforcement data systems, including ALPR databases, must not be used in a manner inconsistent with California law. The California Department of Justice has issued guidance clarifying these restrictions in Information Bulletin No. 2025-DLE-08.

In 2025, the California Legislature passed Senate Bill 274, which would have imposed additional restrictions and oversight. The bill proposed limiting retention periods for non-matching records and expanding state-level review of ALPR use. However, SB 274 was vetoed by Governor Gavin Newsom, who concluded that SB 274 did "not strike the delicate balance between protecting individual privacy and ensuring public safety,... particularly with respect to cold cases."

Collectively, these statutes establish a legal framework that emphasizes transparency, accountability, and restricted data sharing, while placing primary responsibility for compliance on individual law enforcement agencies.

Data Sharing and Side-Sharing

The effectiveness of ALPR systems depends in large part on the ability of LEAs to share data across jurisdictions. Within most ALPR platforms, each agency organizes its cameras into one or more networks that govern both system configuration and data sharing. Agencies may control which other agencies can discover their networks and whether access requests are automatically approved or require explicit authorization. Once access is granted, authorized users from another agency may query shared ALPR data without further approval.

While this model enhances investigative capability—particularly in cases involving vehicles that travel across jurisdictional boundaries—it also places responsibility on each agency to ensure that data sharing practices comply with California law. Civil Code section 1798.90.55(b) provides that a public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law. The SMCCGJ found that data sharing practices vary widely among agencies, with some limiting access to nearby jurisdictions and others permitting broad sharing within the state. The decentralized nature of these sharing controls creates a structural risk: compliance with California law depends not on system-enforced restrictions, but on how individual agencies configure and manage their networks. As a result, even where written policies are compliant, system configurations may permit data sharing practices that are inconsistent with statutory requirements. In general, as the size of a network increases and more law enforcement agencies are granted access, the risk of misuse correspondingly increases.

A related concern is the practice commonly referred to as "side-sharing." For purposes of this report, "side-sharing" refers to the practice in which a California ALPR operator conducts a network query on behalf of an organization that is not authorized to access the data directly—typically an out-of-state or federal agency—and then provides the results outside of the ALPR system. In such cases, audit records reflect that the query was initiated and used by a California agency, when in fact the request originated from, and the results were delivered to, an external entity.

Because the ALPR audit logs reviewed by the SMCCGJ record only the identity of the querying agency and do not capture the ultimate recipient of the data, side-sharing is inherently difficult to detect. Activity that appears compliant on its face may, in fact, circumvent the restrictions imposed by California law, including limitations on sharing ALPR data with entities outside the state.

Side-sharing may involve attempts to access ALPR data outside of established sharing arrangements, including by law enforcement personnel who do not have authorized access. For example, a federal immigration agency may seek to obtain ALPR data from a California jurisdiction in a manner inconsistent with the restrictions imposed by SB 54. Such access could be facilitated by directly contacting personnel within a California LEA and requesting that they conduct an ALPR query on behalf of the external agency.

This issue has been the subject of media reporting and public concern, although verification in specific instances is challenging due to the limitations of available audit data. Media coverage of public statements by certain law enforcement officials has further highlighted the potential risk.

The SMCCGJ found that existing controls to prevent or detect improper data sharing, including side-sharing, are limited. While the ALPR platform provides audit logs, role-based access controls, and, more recently, anomaly detection tools, these features rely on agency-level oversight and do not provide a comprehensive or system-enforced safeguard. There is no centralized mechanism to prevent a user from conducting a query on behalf of an unauthorized entity or to ensure that query results are used solely for authorized purposes.

As a result, compliance with California law in this area depends largely on the policies, training, and oversight practices of individual agencies. In the absence of stronger technical controls or more robust audit capabilities, the risk of unauthorized data access—whether through misconfiguration or side-sharing—remains a significant concern.

Flock Safety

Flock Safety is the largest provider of ALPR systems in the United States and the primary provider of ALPR systems used by LEAs in SMC. The company provides both the physical camera infrastructure and a cloud-based software platform that enables agencies to collect, store, search, and share vehicle detection data. This represents a significant market shift from Vigilant Solutions, who was the most common provider in 2019.

Note that while nearly all ALPR cameras in SMC are provided by Flock, Pacifica also operates 4 Axon mobile cameras that were not investigated by SMCCGJ. Also, ALPR data collected by Flock cameras may also be forwarded to intelligence fusion systems that include other types of surveillance data. Some SMC LEAs use C3.ai, and SMC has recently funded a pilot with Peregrine Systems. These systems are capable of sharing data among agencies and across state boundaries but were not investigated by SMCCGJ and have not received wide media attention.

Flock cameras are typically installed at fixed locations such as major intersections, highways, and entry or exit points to a community. These cameras do not continuously track vehicles; rather, they capture individual "snapshots" or detections as vehicles pass through a camera's field of view. Each detection includes a license plate number, vehicle characteristics (such as make, color, and body type), and metadata including the date, time, and location of the observation.

This information is transmitted to Flock's cloud-based platform, where it is indexed and made searchable. Authorized users access the system through a web-based interface, allowing them to query historical detections or monitor real-time alerts. For example, agencies may create "hotlists" of vehicles of interest—such as stolen vehicles or those associated with criminal investigations—which trigger notifications when detected by any connected camera.

A key feature of the system is its ability to aggregate data across multiple cameras and jurisdictions. While a single camera provides only a point-in-time observation, multiple detections across different locations can allow investigators to infer travel patterns or identify a vehicle's movement over time.

All user activity—including searches, alerts, and administrative actions—is recorded in audit logs. These logs are intended to support oversight and accountability by providing a record of how the system is used. Although Flock hosts the data and provides the technical infrastructure, each customer agency retains control over its own data and is responsible for determining who may access it and under what conditions.

Data Sharing Framework

A defining feature of the Flock platform is its ability to facilitate data sharing among law enforcement agencies. This capability is implemented through a system of configurable "Networks," which function as both administrative groupings and sharing mechanisms. Each agency organizes its cameras into one or more networks and determines whether those networks are visible to other agencies within the platform. When a network is made visible, other agencies may discover it—typically through a map-based interface—and request access.

These access requests are routed to a designated administrator within the owning agency. Depending on how the system is configured, the administrator may review and approve each request individually, or the system may automatically approve requests based on predefined criteria. Once access is granted, users from the approved agency can query the shared data directly, without needing to request permission for each individual search.

This model allows investigators to search for vehicles across jurisdictional boundaries, which can be particularly useful in cases involving regional travel or coordinated criminal activity. At the same time, it introduces complexity, as each agency must determine which other agencies should be granted access and under what conditions.

Agencies can limit sharing in several ways, including restricting access to specific agencies, geographic regions, or operational groupings. Importantly, sharing permissions are not transitive: if Agency A shares data with Agency B, and Agency B shares data with Agency C, Agency C does not automatically gain access to Agency A's data.

Private entities, such as commercial businesses or homeowners' associations, participate in the system differently. Their cameras are not visible within the shared network interface, and they do not independently request access to law enforcement data. Instead, data from private cameras is typically shared directly with local LEAs through arrangements managed with Flock outside the standard user interface.

While this network-based architecture enables collaboration and enhances investigative capabilities, it also places primary responsibility on each agency to manage its sharing relationships in a manner consistent with applicable laws and local policy.

Concerns

Beginning in 2025, a number of media reports and public records analyses brought increased attention to the use of ALPR systems, particularly with respect to how data was being shared among law enforcement agencies. These reports identified instances in which California agencies had configured their systems in a manner that allowed access to ALPR data by out-of-state entities, a practice inconsistent with California law.

Within SMC, the Menlo Park Police Department acknowledged prior instances in which ALPR data had been shared across state lines. Similar issues were identified in other jurisdictions throughout California, suggesting that these were not isolated occurrences but rather reflected broader challenges in how the systems were configured and used.

In addition to concerns regarding system configuration, analysis of audit data highlighted issues related to how queries were conducted and documented. In some cases, users entered generalized descriptions such as "Investigation,"[1] without specifying a particular law enforcement purpose. While such entries are not necessarily improper, they limit the ability of agencies, auditors, and the public to determine whether queries were conducted for authorized purposes.

Taken together, these findings raised questions not only about compliance with legal requirements, but also about the adequacy of system controls and oversight mechanisms. They also underscored the degree to which proper use of the system depends on both technical configuration and user behavior.

System Controls and Vendor Response

In response to these concerns, Flock implemented a series of changes beginning in 2025, aimed at reducing the likelihood of improper data sharing and improving the ability of agencies to monitor system use. These changes reflect a shift from a system that relied heavily on user discretion to one that incorporates more structured controls and constraints.

One of the most significant changes involved restrictions on data sharing across state lines. Prior to 2025, agencies had broad discretion to configure sharing relationships, including the ability to enable "Nationwide" access or establish direct connections with out-of-state agencies. Although such configurations were inconsistent with California law, they were technically permitted within the system.

To address this issue, Flock implemented a phased set of changes. Nationwide sharing was first disabled by default in February 2025 and then permanently removed in March 2025, eliminating the ability for California agencies to broadly expose their data to agencies outside the state. In June 2025, Flock further restricted sharing by disabling the ability to create new out-of-state sharing relationships.

Importantly, these changes did not automatically terminate existing shared relationships. Instead, Flock undertook a process of customer outreach and education, encouraging agencies to review and modify their configurations. As a result, most agencies voluntarily discontinued such arrangements, although some pre-existing relationships remain subject to ongoing legal proceedings. As of this writing, the City of El Cajon is the only California agency with ALPR network sharing relationships extending outside the state. In October 2025, the California Attorney General filed an action against El Cajon alleging non-compliance with SB 34; the case is currently in litigation.

In addition to changes in sharing controls, Flock introduced enhancements aimed at improving how system use is documented and monitored. Historically, users were able to enter free-form text to

[1] Analysis done by the SMCCGJ on all 2025 network queries in California on one SMC LEA's data found that 13.1% of queries entered only "Investigation" as the "Reason" for performing the query.

describe the purpose of a query in a "Reason" field. In practice, this resulted in inconsistent and often vague entries[2], limiting the effectiveness of audit review.

In December 2025, Flock augmented this approach by requiring users to select an "Offense Type" from a standardized list[3] based on National Incident-Based Reporting System (NIBRS) codes. Within California, categories inconsistent with SB 54 are disabled. This change provides a more consistent framework for documenting queries and enables more meaningful analysis of system use. Many agencies have supplemented this requirement by mandating the entry of a case number, linking each query to a specific investigation. This case number is useful for auditing queries within a department but is ineffective for analysis of network queries as LEAs in California do not share a common case management system.

Flock also expanded its audit and monitoring capabilities. Audit logs continue to record all user activity, but additional tools have been introduced to support review. Activity logs track changes to system configuration, including modifications to sharing settings, while the Transparency Portal allows agencies to publish usage statistics and audit summaries.

In April 2026, Flock introduced "Audit Assistance," an automated tool that analyzes system activity and identifies patterns that deviate from an agency's typical usage. These alerts are intended to assist administrators in identifying potential misuse, including unusual query patterns or activity that may warrant further review (side-sharing).

Additional controls have been implemented to restrict system access and reinforce appropriate use. These include limitations on "guest" users outside the agency's domain and role-based access controls that allow agencies to tailor system permissions based on user responsibilities. Flock's terms of service also prohibit use of the system on behalf of unauthorized individuals or agencies.

While these changes represent meaningful improvements, they are primarily designed to support and guide user behavior rather than to enforce compliance directly. As such, their effectiveness depends on how agencies configure and use the system.

Training and Compliance Support

Flock provides training on system operation, legal use, and compliance requirements as part of its onboarding process. Agencies may supplement this training with local policies, procedures, and internal controls tailored to their operational environment. While these resources support compliance, they do not substitute for agency responsibility to ensure that system use is consistent with applicable laws and policies.

Remaining Limitations

Notwithstanding these enhancements, important limitations remain in the system's ability to prevent or detect improper use.

First, while audit logs provide a record of which agency conducted a query and when it occurred, they do not capture how the resulting information is ultimately used or shared. This means that even

[2] The search reason "warrant" could refer to a warrant issued by a California judge for an authorized law enforcement purpose, or alternatively to an administrative warrant issued by a federal agency such as ICE. Numeric strings typically correspond to sections of California penal code, but many LEA's listed a crime category such as "theft" or "burglary". The SMCCGJ found no accepted usage of the "Reason" field across or even within LEAs.

[3] A list of these offense codes is provided in Appendix A.

where a query appears appropriate on its face, there is no direct way to determine whether the results were subsequently provided to an unauthorized party.

Second, the system does not technically prevent a user from conducting a query on behalf of another individual or agency (side-sharing). Although such conduct may violate policy or law, it is not inherently detectable through system controls alone. As a result, certain forms of misuse—particularly those involving indirect access—are difficult to identify through audit data.

Finally, the effectiveness of audit and monitoring tools depend on active review by agency personnel. Identifying potential issues requires not only access to audit data but also the time, expertise, and judgment to interpret that data. This introduces variability in how different agencies monitor system use and respond to potential concerns.

These limitations illustrate that, while system-level controls can reduce risk, they cannot fully eliminate it. Effective oversight requires a combination of technical controls, clear policies, and consistent enforcement.

Conclusion

Flock has implemented a number of substantive changes to its platform in response to concerns regarding data sharing and legal compliance. These changes have improved transparency, standardized key aspects of system use, and provided agencies with additional tools to monitor activity.

At the same time, the system continues to rely heavily on agency-level decisions regarding configuration, access, and oversight. Certain risks—particularly those associated with indirect or unauthorized use—cannot be fully mitigated through system design alone.

As a result, responsibility for ensuring compliance with Civil Code sections 1798.90.5 through 1798.90.55 ultimately rests with each individual law enforcement agency. The effectiveness of the system, therefore, depends not only on the capabilities of the technology but also on how it is implemented and governed at the local level.

METHODOLOGY

To determine whether ALPR operators in SMC comply with applicable California law and whether their practices align with their adopted ALPR policies, the SMCCGJ began by reviewing the content available on the public websites of each LEA in the County. Most LEA websites include information regarding ALPR usage and transparency, often with a link to the agency's Flock Transparency Portal, which is maintained by Flock on behalf of its customers.

The SMCCGJ issued document requests to all ALPR operators in SMC, seeking ALPR policies, recent audit reports, current Flock contracts, and any supporting documentation demonstrating compliance with California law and agency policy. Findings based on nonproduction reflect the absence of responsive records produced to the SMCCGJ, not a conclusive determination that no responsive record exists.

The SMCCGJ was able to identify an ALPR policy document for every SMC ALPR operator, which guided the examination of compliance with that policy. For some operators we were provided an organization audit report, which lists all ALPR queries initiated within that LEA. The organization audit was visually reviewed in a spreadsheet, which is feasible for what is at most a few hundred rows. Some operators provided a network audit report, which lists all ALPR queries initiated by

other Flock customers on that operator's data. As the network audit report can be quite large (upwards of 25,000/month), analysis of this data was carried out by first loading it into a database.[4]

The SMCCGJ examined network sharing reports from the operators that provided them. This information is also publicly available through Flock Safety's Transparency Portal. The network sharing reports identify the agencies and entities with which each operator shares ALPR data.

The SMCCGJ conducted interviews with several LEAs in SMC, with representatives of Flock, and with the Northern California Regional Intelligence Center (NCRIC).The SMCCGJ collected media reports related to ALPR implementations in SMC, in the state of California, and nationwide.

DISCUSSION

Public Interest

Issues related to the use of ALPR systems have received significant public attention in both SMC and throughout California. Several communities within the County have debated canceling their ALPR contracts or exploring alternative provider. As of this date, all have decided to continue operations with Flock. An article on ALPR usage published by Palo Alto Online on December 29, 2025, was the publication's most-downloaded article of the year.

For the general public, it can be difficult to determine the root cause of security breaches reported in the media. Coverage has variously attributed these incidents to product design limitations, accidental or intentional misconfiguration, and inadequate operator training. As discussed earlier in this report, ALPR system functionality has evolved in response to public concerns, with enhancements intended to facilitate compliance with applicable laws.

Sharing Within San Mateo County

This investigation found that the extent of data sharing among SMC ALPR operators varies significantly, with the number of network sharing relationships ranging from three in Woodside to 335 in San Bruno. During the course of this investigation, one SMC operator reduced the scope of their network sharing after evaluating the public safety value of broader data access against local privacy considerations. Some LEAs felt that broad access was valuable in addressing the pattern of crimes committed in their community. Others felt that sharing too broadly would not solve more crimes and could risk losing the support of their local community.

As of December 2025, no SMC operators were found to be sharing ALPR data with entities outside California. The investigation did identify instances in which SMC operators shared ALPR data with private organizations, specifically security agencies serving Stanford University and University of the Pacific. Under Civil Code section 1798.90.55(b), a public agency may share ALPR information only with another "public agency" and only as otherwise permitted by law. The materials produced did not establish that the private university security recipients meet the definition of a "public agency" or that an applicable statutory exception authorizes the sharing. It remains the responsibility of each LEA to determine whether such entities qualify as public agencies under applicable law. If deemed public agencies, these entities would be subject to the same statutory and policy requirements governing ALPR use.

[4] The network audit report was delivered in comma-separated value format, was then bulk-loaded into a MySQL database and then queried using the Structured Query Language.

The table below summarizes these findings.

Operator	Network Shares 2/26/2026	Network Shares 4/13/2026	Private University Security Shares 4/13/2026	Apparent Sharing Guideline
Atherton	315	317	2	
Belmont	157	145	2	Adjacent Counties
Brisbane	93	92	1	50-mile radius
Burlingame	Not available	357	2	
Colma	321	326	2	
Daly City	Not available	Not available	not available	Flock portal is not enabled.
East Palo Alto	303	308	2	
Foster City	Not available	Not available	Not available	Flock portal excluded network sharing report.
Half Moon Bay	Not available	290	0	
Hillsborough	303	318	2	
Menlo Park	247	242	1	
Pacifica	276	283	2	
Redwood City	102	100	1	Bay Area Counties
San Bruno	331	335	2	
San Mateo	283	280	0	
San Mateo County Sheriff's Office	299	300	2	Reduced in February to adjacent Counties.
South San Francisco	15	15	0	San Mateo County
Woodside	3	3	0	Adjacent towns

Public Commentary

Under Civil Code section 1798.90.55(a), a public agency that operates an ALPR system must provide the opportunity for public comment. The SMCCGJ did not identify any instances in which ALPR cameras were deployed without the required public notice and discussion.

ALPR Policies

California law requires each ALPR operator to adopt a written ALPR policy and to post that policy in a conspicuous manner (Civ. Code, §§ 1798.90.53(a)–(b); 1798.90.51 (a)–(b)). The California Department of Justice provides a model ALPR policy template, which agencies may adopt or

modify. Some departments also utilize policy templates developed by Lexipol, a provider of standardized law enforcement policy materials.

The following section evaluates each SMC law enforcement agency's ALPR policy, including whether it is conspicuously posted, and assesses whether the agency's actual operations are consistent with its stated policy.

Summary Matrix of ALPR Policy and Operational Findings

Policy Posting and Currency. Most LEAs and police departments provided an ALPR policy in response to the SMCCGJ document request. The SMCGJ reviewed each policy for alignment with the policy templates and guidance provided by the State of California and Lexipol. The SMCCGJ also reviewed each department's public website to determine whether the policy was conspicuously posted in accordance with California DOJ guidance 2023-DLE-06, and whether the publicly posted version matched the version provided in response to the document request.

Audit Practices. The SMCCGJ requested copies of recent audit reports from each LEA. Where an audit frequency was specified in an agency's ALPR Policy, the SMCCGJ reviewed the materials provided to determine whether audits appeared to have been conducted at the stated intervals. The SMCCGJ also examined the contents and scope of each audit report.

For purposes of this investigation, a "strong" audit is one that substantiates compliance with both applicable California law and each material element of the LEA's stated ALPR Policy. California law requires a policy to describe monitoring and "a process for periodic system audits," but does not prescribe a uniform audit report format or methodology. The labels "strong," "partial," and "weak" are assessment terms used in this report and are not statutory classifications.

In the absence of meaningful audit controls, the public has limited assurance that an agency's stated policies are being consistently implemented in practice. By contrast, a "weak" audit examines only selected legal or policy elements and does not comprehensively evaluate operational compliance.

Finally, the SMCCGJ reviewed whether audit reports were made available to the public or presented to the relevant city, town, or county governing body.

Data Retention. Civil Code section 1798.90.51(b)(2)(D) requires each ALPR policy to specify a data retention period after which ALPR data will be deleted unless it is associated with an active investigation or otherwise retained pursuant to law. The SMCCGJ compared the retention period stated in each agency's ALPR policy with the retention period displayed on Flock's Transparency Portal and, where available, the retention provisions contained in the agency's Flock contract. Matching retention periods were classified as "consistent," while differing retention periods were classified as "inconsistent." We did not examine in detail the process by which Flock deletes data after the stated retention period, as this topic has been addressed by third-party audits.

Data Sharing Process. Each policy must describe criteria and a process for sharing ALPR data. We examined this statement to ensure that it prohibits the sale of ALPR data, out-of-state sharing, sharing to private parties, and usage for other than valid law enforcement purposes. We examined any written guidelines and processes for receiving and approving requests for sharing data, and for any documentary evidence supporting the implementation of that process. Most policies included the sharing process description and documented from templates, but our interviews and document requests did not find an LEA who followed the process described in this "Template." Several LEAs described the sharing process provided by the Flock platform, which is what we heard described

during interviews as the adopted process. The LEAs with outdated policies described an outdated sharing process mediated by NCRIC. No LEA's policy described guidelines for ALPR data sharing within California, though several outlined coherent criteria for what sharing requests to approve.

Contract Terms. The SMCCGJ reviewed the 14 Flock contracts provided in response to its document requests. One contract included an addendum with California compliance provisions ("CA terms") requiring Flock to adhere to California law governing the protection, access, and disclosure of ALPR data maintained on behalf of California LEA customers, consistent with recommendations previously issued by the California State Auditor.

The absence of express contractual compliance terms does not itself establish a violation of California law, which applies regardless of contract language. In this report, the presence or absence of such terms is evaluated as an additional contractual compliance control.

The table below summarizes the SMCGJ's assessment of ALPR policy compliance and operational alignment among LEAs in SMC.

Agency	Policy Posting / Currency	Audit Practices	Data Retention	Data Sharing Process	Contract Terms
Atherton	Not conspicuous; current, but with multiple versions	Strong; published in Council Minutes	Inconsistent	Template	No CA terms
Belmont	Conspicuous; current	Strong; not published	Consistent	Flock	No CA terms
Brisbane	Not conspicuous; current	Audit reports not provided	Consistent	Template	No CA terms
Burlingame	Not conspicuous; current	Audit reports not provided	Consistent	Template	Contract not provided
Colma	Not conspicuous; current	Strong; not published	Inconsistent	Template	CA terms included in addendum
Daly City	Conspicuous, outdated (NCRIC references)	Strong, regular audit; not published	Inconsistent	Outdated	No CA terms
East Palo Alto	Conspicuous; current	Partial; publicly posted	Consistent	Not described	No CA terms

Agency	Policy Posting / Currency	Audit Practices	Data Retention	Data Sharing Process	Contract Terms
Foster City	Conspicuous; current, but broken link to policy	Audit reports not provided.	Inconsistent	Template	No CA terms
Hillsborough	Not conspicuous; Outdated (NCRIC references)	Audit reports not provided.	Consistent	Outdated	No CA terms
Menlo Park	Not conspicuous; current	Weak; published in City Council minutes.	Consistent	Template	No CA terms
Pacifica	Conspicuous; current	Brief, but strong; not published	Consistent	Flock	Contract not provided
Redwood City	Conspicuous, outdated (NCRIC references)	Strong; not published	Inconsistent	Outdated	No CA terms
San Bruno	Conspicuous; current	Partial; not published	Consistent	Flock	No CA terms
San Mateo	Conspicuous; current	Weak; not published	Consistent	Template	No CA terms
SMC Sheriff's Office	Conspicuous; current	Partial; published in BOS minutes.	No stated retention	Template	No CA terms
South San Francisco	Conspicuous; current	Partial; not published.	Consistent	Template	No CA terms
Woodside	Conspicuous (via SMC SO) and current	Strong; published in Town Council minutes	Consistent	Template	Contract not provided.

As shown above, while several agencies demonstrate strong alignment between policy and operational practices, others exhibit deficiencies in audit procedures, inconsistencies in stated data retention practices, and incomplete or inaccurate documentation of data-sharing processes and decisions. These findings highlight the absence of standardized ALPR governance and oversight practices across SMC.

FINDINGS

This section summarizes findings based on evidence produced or otherwise reviewed by the SMCCGJ. The accompanying table identifies the findings assigned to the governing body of each LEA based on the evidence described in this report.

F1. The ALPR operator's ALPR policy was not posted in a manner that appears consistent with the California Attorney General's guidance on "conspicuous" posting.

F2. The ALPR operator's ALPR Policy appears to be outdated because it describes ALPR operations as mediated by NCRIC, a practice the investigation found was discontinued several years ago.

F3. The ALPR operator shared ALPR information with private university security entities but did not establish that the receiving entity was a "public agency" as defined in Civil Code section 1798.90.55(b), or that the sharing was otherwise permitted by law within the meaning of Civil Code section 1798.90.55(b).

F4. The ALPR operator did not produce records demonstrating that audits required by its ALPR policy had been conducted.

F5. The audit reports produced by the ALPR operator were insufficient to substantiate compliance with applicable California law and the operator's published ALPR policy.

F6. The ALPR operator's Flock Safety contract does not include provisions specifically requiring compliance with applicable California ALPR laws.

F7. The operator's ALPR policy described a process requiring written requests and executed agreements for ALPR data-sharing relationships; however, the records produced did not substantiate that this process was followed or that the required agreements were obtained.

F8. The operator's ALPR policy did not establish criteria governing the approval of in-state ALPR data-sharing requests or the termination of existing network-sharing relationships.

F9. The retention period specified in the operator's ALPR Policy does not match the retention period as reported by the Flock transparency portal or Flock contract.

RECOMMENDATIONS

While the recommendations below are generally applicable to all LEAs in SMC, some recommendations have already been implemented by some LEAs. The accompanying table identifies the recommendations directed to the governing body of each LEA reviewed by the SMCCGJ.

R1. The ALPR operator should conspicuously post the current version of their ALPR Policy as required by Civil Code sections 1798.90.51(a)–(b).

R2. The ALPR operator with outdated ALPR policies should revise those policies to accurately reflect current operational practices.

R3. The ALPR operator currently identified as sharing ALPR data with private university security entities should obtain and retain a written legal and factual determination that the recipient is a "public agency" under Civil Code section 1798.90.5(f), or that the sharing is otherwise permitted by law; if no lawful basis exists, the operator should terminate the sharing relationship.

R**4.** The ALPR operator should prepare audit reports in accordance with the frequency stated in the operator's published ALPR policy.

R5. The audit reports produced by the ALPR operator should substantiate compliance with applicable California law and the operator's published ALPR policy.

R6. Upon contract renewal, the ALPR operator should incorporate contractual language requiring vendor compliance with applicable California law and prohibiting vendors from disclosing ALPR data to unauthorized third parties. Operators should consider provisions similar to those contained in the Town of Colma contract with Flock.

R7. The ALPR operator should update its ALPR policy to accurately reflect the process used to approve ALPR data-sharing relationships.

R8. The ALPR operator should include in their ALPR policies written criteria governing the approval, denial, periodic review, and termination of in-state ALPR network-sharing relationships.

R9. The ALPR operator should update their ALPR policy or Flock contract terms, as necessary, so that the stated retention rule accurately reflects operations.

REQUEST FOR RESPONSES

Pursuant to Penal Code 933.05, the Civil Grand Jury requests responses from the following governing bodies:

Respondent	Findings	Recommendations
Atherton Town Council	F1, F3, F6, F7, F8, F9	R1, R3, R6, R7, R8, R9
Belmont City Council	F3, F6, F8	R3, R6, R8
Brisbane City Council	F1, F3, F4, F5, F6, F7, F8	R1, R3, R4, R5, R6, R7, R8
Burlingame City Council	F1, F3, F4, F5, F6, F7, F8	R1, R3, R4, R5, R6, R7, R8
Colma City Council	F1, F3, F5, F7, F8, F9	R1, R3, R5, R7, R8, R9
Daly City City Council	F3, F6, F7, F8, F9	R3, R6, R7, R8, R9
East Palo Alto City Council	F3, F5, F6, F7, F8	R3, R5, R6, R7, R8
Foster City City Council	F3, F4, F5, F6, F7, F8, F9	R3, R4, R5, R6, R7, R8, R9
Half Moon Bay Town Council	F3, F5, F6, F7, F8, F9	R3, R5, R6, R7, R8, R9
Hillsborough Town Council	F1, F2, F3, F4, F5, F6, F7, F8	R1, R2, R3, R4, R5, R6, R7, R8
Menlo Park City Council	F1, F3, F5, F6, F7, F8	R1, R3, R5, R6, R7, R8
Millbrae City Council	F3, F5, F6, F7, F8, F9	R3, R5, R6, R7, R8, R9
Pacifica City Council	F3, F5, F6, F8	R3, R5, R6, R8
Portola Valley Town Council	F3, F5, F6, F7, F8, F9	R3, R5, R6, R7, R8, R9
City Council of Redwood City	F2, F3, F5, F6, F7, F8, F9	R2, R3, R5, R6, R7, R8, R9
San Bruno City Council	F4, F5, F6, F7, F8	R4, R5, R6, R7, R8
San Carlos City Council	F3, F5, F6, F7, F8, F9	R3, R5, R6, R7, R8, R9

Respondent	Findings	Recommendations
Ken Binder, San Mateo County Sheriff	F3, F5, F6, F7, F8, F9	R3, R5, R6, R7, R8, R9
San Mateo City Council	F4, F5, F6, F7, F8	R4, R5, R6, R7, R8
South SF City Council	F5, F6, F7, F8	R5, R6, R7, R8
Woodside Town Council	F5, F6, F7, F8	R5, R6, R7, R8

RESPONSE REQUIREMENTS

California Penal Code Section 933.05 provides as follows (emphasis added):

(a) For purposes of subdivision (b) of Section 933, as to each grand jury finding, the responding person or entity shall report one of the following:

(1) The respondent **agrees** with the finding.
(2) The respondent **disagrees** wholly or partially with the finding, in which case the response shall **specify the portion of the finding that is disputed and shall include an explanation of the reasons therefor**.

(b) For purposes of subdivision (b) of Section 933, as to each grand jury recommendation, the responding person or entity shall report one of the following actions:

(1) The recommendation has been implemented, **with a summary regarding the implemented action**.
(2) The recommendation has not yet been implemented, but will be implemented in the future, **with a timeframe for implementation**.
(3) The recommendation requires further analysis, **with an explanation and the scope and parameters of an analysis or study, and a timeframe for the matter to be prepared for discussion by the officer or head of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This timeframe shall not exceed six months from the date of publication of the grand jury report**.
(4) The recommendation will not be implemented because it is not warranted or is not reasonable **with an explanation therefor.**

Under Penal Code section 933(c), the governing body of a public agency must respond within 90 days after the grand jury submits its final report, and an elected county officer or agency head for which the grand jury has responsibility under Penal Code section 914.1 must respond within 60 days regarding matters under that officer's or agency head's control.

BIBLIOGRAPHY

Automated License Plate Readers, Report 2019-118, California State Auditor, February 2020.

California Automated License Plate Reader Data, 2023-DLE-06, California Department of Justice.

National Crime Information Center Administration of Warrants, 2025-DLE-08, California Department of Justice, April 7, 2025.

A Delicate Balance: Privacy vs. Protection, Report of the San Mateo County Civil Grand Jury, 2016–2017.

FOOTNOTES

1 Analysis done by SMCCGJ on all 2025 network queries in California on one SMC LEA's data found that 13.1% of queries entered only "Investigation" as the Reason for performing the query.

2 The search reason "warrant" could refer to a warrant issued by a California judge for an authorized law enforcement purpose, or alternatively to an administrative warrant issued by a federal agency such as ICE.

3 A list of these offense codes is provided in Appendix A.

4 The network audit report was delivered in comma-separated value (CSV) format, bulk-loaded into a MySQL database and analyzed using the Structured Query Language (SQL).

5 https://www.paloaltoonline.com/police/2025/11/05/east-palo-alto-leaders-push-back-on-license-plate-readers-amid-privacy-concerns/

6 https://www.coastsidenews.com/news/half-moon-bay-to-revisit-license-plate-reader-program-and-ice-policies/

7 https://www.almanacnews.com/news/2025/12/29/the-years-biggest-stories/

Appendix A - Flock Safety Offense Types

Flock Safety

Agency Specific Settings

Depending on your agency's settings, searches may also require Search Reason or Case Number. These settings are chosen by your administrator and should align with your agency's LPR Policy.

All Available Offense Types

- Animal Offenses (cruelty/neglect)
- Arson
- Assault/Battery Offenses
- Assault/Battery Offenses (Domestic)
- Bribery
- Burglary/Breaking & Entering
- City Planning/Traffic Analysis
- Child Abuse/Neglect
- Counterfeiting/Forgery
- Criminal Motor Vehicle Offense (incl. Road Rage/Reckless)
- Curfew/Loitering/Vagrancy Violations
- Destruction/Damage/Vandalism of Property
- Disorderly Conduct/Disturbance
- Driving Under the Influence (DUI/DWI/OWI/OVI)
- Drugs/Narcotics
- Extortion/Blackmail
- Financial Crime (Embezzlement/Fraud)
- Gambling
- Hit and Run/Car Accident
- Homicide/Death Investigation
- Human Trafficking
- Illegal Dumping/Littering
- Immigration (civil/administrative)
- Immigration (criminal)
- Indecent Exposure/Lewd
- Juvenile Delinquency
- Kidnapping/Abduction
- Larceny/Theft Offenses
- Alcohol Offenses (Non-DUI)
- Material Witness
- Missing/Endangered Person/Runaway
- Motor Vehicle Theft/Stolen
- Obstructing the Police (Fleeing/Eluding)
- Obstructing Justice
- Pornography/Obscene Material
- Prostitution
- Disturbing Public Peace/Riot
- Robbery
- Secured Area Access Control
- Sex Offenses
- Stalking
- Stolen Property Offenses
- Terrorism/Terroristic Threats
- Threats/Harassment
- Traffic Infraction
- Trespass
- Wanted Person (Arrest Warrant/Fugitive)
- Weapons Offense (Guns/Shots Fired)
- Property Recovery (Civil Enforcement)
- Protective/Protection Order
- Welfare Check

flocksafety.com (866) 901-1781 | support@flocksafety.com