**MARIN COUNTY CIVILIAN OVERSIGHT COMMISSION**

**MEMORANDUM: FINDINGS AND RECOMMENDATIONS REGARDING FLOCK SAFETY ALPR TECHNOLOGY**

**TO:** Marin County Sheriff

**FROM:** Civilian Oversight Commission

**DATE:** 11-16-26

**SUBJECT:** Findings and Recommendations Regarding Flock Safety Automated License Plate Reader Technology

## 1. Executive Summary

The Marin County Civilian Oversight Commission (the "Commission") has conducted a review of the Marin County Sheriff's Office's (MCSO) use of Flock Safety Automated License Plate Reader (ALPR) technology. This review included MCSO policies and procedures, available usage and audit records, data-sharing practices, relevant California laws, the 2022 settlement concerning ALPR information sharing, and information provided by MCSO and community subject-matter experts. The Commission also examined reports of unauthorized or improper access to ALPR information in other jurisdictions using the Flock Safety platform.

The review identified significant concerns regarding data security, MCSO's control over collected information, the effectiveness of auditing practices, and transparency. Particularly concerning are the reported unauthorized access to Marin ALPR information during 2024 and MCSO's acknowledgment that it cannot independently verify the legitimacy of individual searches conducted by outside agencies authorized to access its information.

Similar incidents involving Flock systems in other California jurisdictions raise broader questions about whether local agencies can reliably prevent unauthorized access when information is maintained within a vendor-managed, interconnected network.

The Commission recognizes the legitimate investigative benefits of ALPR technology. However, those benefits do not eliminate the obligation to protect sensitive information collected about members of the public.

**The Commission recommends that MCSO immediately suspend its use of Flock Safety ALPR technology unless and until independent technical verification demonstrates that the system can reliably prevent unauthorized access and sharing.**

The Commission further recommends stronger requirements governing data control, auditing, procurement, and transparency for any future ALPR system.

## 2. Key Findings

### A. Previous Information-Sharing Restrictions Have Not Resolved the Underlying Concern

In 2022, MCSO entered into a settlement agreement following litigation concerning the sharing of ALPR information with federal and out-of-state agencies. The settlement established restrictions intended to prevent prohibited sharing and was accompanied by changes to departmental policy.

The settlement concerned MCSO's earlier ALPR arrangements rather than the Flock platform currently under review. Nevertheless, the reported unauthorized access involving Flock in 2024 raises a critical question: **Can MCSO ensure compliance with legal and policy restrictions when the technical mechanisms governing access to its information are managed through an outside vendor's network?**

Written policies and settlement obligations are necessary, but their existence does not establish that prohibited access is technically prevented.

### B. Unauthorized Access Raises Concerns About the Flock Platform

Recent reporting indicates that federal and out-of-state agencies improperly accessed or searched ALPR information associated with Marin County during 2024. MCSO has reportedly acknowledged discovering unauthorized access in late 2024 and taking steps to disable it.

The Commission also reviewed incidents involving Flock systems in other California jurisdictions.

In San Francisco, a departmental audit identified improper searches conducted on behalf of federal and out-of-state agencies through a regional intelligence-sharing arrangement. San Francisco officials reported that those agencies did not directly access the city's Flock system, illustrating how information may become accessible through indirect pathways even when direct access is restricted.

These incidents do not necessarily involve identical technical failures. However, they raise concerns about whether the platform's access controls, sharing arrangements, and network architecture can consistently enforce the restrictions established by individual California agencies.

The central issue is not simply whether MCSO has adopted appropriate policies or configured particular settings. It is whether MCSO can independently control and verify every authorized pathway through which information collected by its cameras may be accessed.

**C. Limited Oversight of Searches Conducted by Outside Agencies**

During a meeting with the Commission, MCSO explained that outside law enforcement agencies must first establish a Memorandum of Understanding (MOU) before being granted access to MCSO's ALPR information.

However, MCSO also acknowledged significant limitations in its ability to monitor and audit searches conducted by those agencies. According to MCSO, the information available to the department is limited to the jurisdiction conducting the search, the networks searched, and the time of the search.

MCSO does not have access to the identity of the individual conducting the search, the associated case number, the license plate searched, the information returned, or the reason for the search.

Consequently, MCSO cannot independently determine whether individual searches conducted by outside agencies are associated with legitimate investigations or otherwise comply with applicable access and sharing restrictions.

**The Commission finds that requiring an MOU before granting access is an important administrative safeguard, but it does not provide meaningful accountability if MCSO cannot independently verify how its information is subsequently accessed and used.**

**D. Limitations of Existing Auditing Practices**

During its meeting with the Commission, MCSO explained that it conducts monthly in-depth audits of approximately 5–10 randomly selected ALPR searches. According to MCSO, these audits include verifying that the case number and investigative purpose associated with each search are legitimately connected to the underlying investigation.

The Commission recognizes the value of these substantive audits. However, given the volume of searches conducted through the Flock system, a monthly sample of 5–10 searches is insufficient to establish, with meaningful statistical confidence, that improper searches occur at an acceptably low rate.

While MCSO described the selection as random, the Commission has not evaluated the methodology used to select the searches.

The Commission therefore recommends a documented, statistically valid sampling methodology that determines the appropriate monthly sample size based on actual search volume, a 95% confidence level, and a target improper-search rate below 1%.

Additionally, MCSO's limited access to information regarding searches conducted by outside agencies prevents similarly substantive verification of those searches, creating a separate accountability concern.

**Even comprehensive auditing is not a substitute for preventive security controls.** Audits may detect unauthorized access after it occurs; they do not necessarily prevent the access itself.

**E. Transparency and Accountability**

Although MCSO reportedly became aware of the 2024 unauthorized access in late 2024, the incident did not become publicly known until 2026.

This delay raises concerns about the timely disclosure of significant privacy and security incidents, particularly while the Civilian Oversight Commission was reviewing MCSO's ALPR practices.

Effective civilian oversight depends on timely access to information concerning material policy violations, security incidents, and corrective actions. Such disclosure should be governed by clear requirements rather than discretionary reporting practices.

**3. Formal Recommendations**

**Recommendation 1. Immediately Suspend Flock Safety ALPR Use**

The Commission recommends that MCSO immediately discontinue operational use of ALPR technology, including the Flock Safety technology currently in use.

The discontinuation of all ALPR use should remain in effect unless and until independent technical verification demonstrates that the system can reliably prevent unauthorized access and sharing, consistent with California law, MCSO policy, and applicable contractual obligations.

Verification should address the platform's underlying network architecture, third-party access pathways, sharing permissions, and effectiveness of technical restrictions, rather than relying exclusively on vendor assurances or departmental policy.

Revised policies, additional training, increased auditing, or changes to system settings should not, by themselves, be considered sufficient grounds for reinstating Flock.

MCSO should also evaluate alternative ALPR technologies capable of meeting the County's security, privacy, and accountability requirements.

**Recommendation 2. Require Direct County Control Over ALPR Information**

MCSO should prioritize ALPR systems that maintain collected information within infrastructure directly controlled by the County, preferably stored locally rather than within a vendor-managed nationwide data-sharing network.

Any future system should demonstrate that:

- MCSO retains effective control over access to its information.
- Outside agencies cannot access or query County information without explicit lawful authorization.
- Vendors cannot independently grant access or bypass County restrictions.
- All access pathways and sharing permissions are independently verifiable.

Physical storage location alone should not establish compliance. The determining requirement must be meaningful, technically enforceable County control.

**Recommendation 3. Require Complete and Verifiable System Logs**

Any future ALPR system should maintain complete, tamper-evident logs documenting searches conducted by MCSO personnel and outside agencies.

At minimum, these records should identify the individual user and agency, date and time, license plate queried, investigative purpose, associated case or incident number, information returned or shared, and relevant system-permission changes.

MCSO and authorized independent auditors must be able to access and verify these records without relying solely on vendor-generated summaries.

Records should be retained for a period sufficient to support compliance reviews, investigations, and applicable legal obligations.

**Recommendation 4. Establish Statistically Valid Monthly Audits**

MCSO should adopt a written policy requiring monthly audits based on a documented, statistically valid sampling methodology.

The methodology should:

- Use a random sample calculated from the actual monthly search volume.

- Aim to provide 95% statistical confidence that the improper-search rate is below 1% when no improper searches are identified.
- Document the random selection process and make it independently verifiable.
- Permit alternative methodologies providing equivalent or stronger statistical assurance, subject to independent validation.
- Verify the legitimate investigative connection between each sampled search and its supporting case or incident records.
- Include substantive auditing of outside-agency searches and targeted reviews of unusual activity, complaints, and suspected violations.
- Document findings, corrective measures, and follow-up reviews.

The methodology should specify how results are evaluated when improper searches are identified and how additional review is triggered.

Auditing of third-party access, system permissions, and security incidents should supplement the search-sampling process rather than be limited to that sample.

**Recommendation 5. Provide Independent Audit Oversight**

ALPR audits should be subject to meaningful independent review by the Inspector General, an appropriate County auditing function, or another qualified independent entity.

The reviewing entity should have access to underlying records and sufficient technical expertise to assess compliance without relying exclusively on MCSO or vendor representations.

Significant findings and corrective actions should be reported to the Commission, consistent with applicable confidentiality requirements.

**Recommendation 6. Strengthen Future ALPR Procurement Requirements**

Any future ALPR procurement or contract should include enforceable requirements addressing:

- Vendor compliance history and previously identified security deficiencies.
- County control of collected information and restrictions on vendor and third-party access.
- Independently verified technical safeguards and system architecture.

- Complete audit records and independent inspection rights, including records of outside-agency searches.
- Data retention, deletion, and security incident notification.
- Corrective-action requirements, contractual remedies, and termination rights.

An independent privacy and security assessment should be completed before any new system becomes operational.

**Recommendation 7. Establish Mandatory Incident Notification and Disclosure**

MCSO should adopt a written policy requiring timely reporting of material ALPR privacy, security, or unauthorized-access incidents to appropriate County officials, the Inspector General, and the Civilian Oversight Commission.

The policy should establish notification timelines, documentation requirements, and procedures for public disclosure consistent with applicable law.

MCSO should also provide the Commission with a written accounting of the 2024 incident, including when the department became aware of the issue, the corrective measures taken, and the circumstances surrounding the delay in public disclosure.

**4. MCSO Response and Commission Consideration**

This memorandum represents the Commission's findings and recommendations and is being provided to MCSO for consideration.

MCSO was afforded three weeks to provide a written response, identify any factual inaccuracies, submit relevant supporting information, and respond to the proposed recommendations, before the Commission adopted these findings on November 16, 2026.

**5. Conclusion**

The Commission recognizes that ALPR technology can provide legitimate investigative benefits. However, collecting information concerning the movements of members of the public requires safeguards that are effective in practice, not simply established in policy.

Despite existing legal restrictions, departmental policies, and information-sharing agreements, the reported unauthorized access involving Flock, together with similar incidents in other jurisdictions and MCSO's acknowledged limitations in auditing outside-agency searches, raises serious questions about whether the current platform can reliably enforce those restrictions.

The Commission therefore recommends suspending Flock until its technical safeguards can be independently verified and establishing stronger standards for any future ALPR technology.

**The fundamental requirement is that MCSO must be able to demonstrate meaningful control over the information it collects and reliably prevent access that California law and departmental policy prohibit.**