

CLETS vs. Flock Safety: Two Systems, Two Standards of Accountability

A statewide comparison for California residents and advocates. Verify against your city's specific contract before citing locally.

Category	CLETS -- California Law Enforcement Telecommunications System	Flock Safety -- Private Vendor ALPR Network
Who runs it	STATE AGENCY. Managed by the California Dept. of Justice -- accountable to the legislature, the Attorney General, and the public.	PRIVATE COMPANY. Managed by Flock Group Inc., a venture-backed company valued at \$7.5B. Accountable to investors, not residents.
Who can access it	STRICTLY CONTROLLED. Authorized law enforcement and criminal justice personnel only, on a strict need-to-know / right-to-know basis defined by state law.	POORLY AUDITED. No warrant required to query data. Multiple California cities discovered inactive accounts and unauthorized federal access -- often through vendor audits, not their own oversight.
Penalty for unauthorized access	FELONY EXPOSURE. Govt. Code 6200 and Penal Code 11141-11143: 16 months to 3 years in state prison, fines up to \$10,000, termination, loss of licenses. DOJ and AG investigate.	PRESS RELEASE. No criminal penalties for vendor configuration errors. Cities bear the legal risk. Flock issues statements and continues operating under the same contract.
Audit trail	MANDATORY AND PUBLIC. Agencies must report misuse annually to the California AG. Audit records are subject to public oversight.	EXISTS BUT HIDDEN. Audit logs exist but are frequently withheld as investigative documents exempt from public records requests. Sensitive fields masked even from local departments.
Federal agency access	CONTROLLED VIA LAW. Access governed by California and federal statute. Unauthorized sharing is itself a criminal offense.	BYPASSED BY VENDOR. Oxnard, Ventura County, San Francisco, Mountain View, and Los Altos all discovered federal access without their knowledge despite "California only" settings. SF: 1.6M unauthorized queries in 7 months.
Public / council oversight	LEGISLATIVE OVERSIGHT. Governed by state statute. Any changes to access rules, retention, or data sharing require legislative action or AG guidance.	FREQUENTLY BYPASSED. AB 481 requires council approval for surveillance tech. Multiple California cities report contract expansions added without council votes or public hearings.
Data retention	DEFINED BY STATUTE. Retention policies set by California law, not contract negotiation with a private vendor.	CONTRACT-DEFINED. Typically 30 days per vendor FAQ, with supervisor-approved extensions. No independent verification that extensions are tracked or limited.
When it goes wrong	OFFICERS FACE PROSECUTION. Fired, prosecuted, forced to resign. DOJ investigates. Criminal charges apply regardless of whether the officer profited.	VENDOR APOLOGIZES. Flock issues a statement and continues operating. Richmond CA had to negotiate a \$290,000 per-incident penalty clause just to get basic protections in writing.
Real-world officer misuse	PROSECUTED UNDER EXISTING LAW. CLETS misuse results in criminal charges, termination, and civil liability under well-established California statutes.	DOCUMENTED AND GROWING. Costa Mesa officer pleaded guilty to using Flock to stalk his mistress and her romantic interests. Similar cases in WI, FL, KS, and GA -- including two police chiefs.

Sources: CA Govt. Code 6200; Penal Code 11141-11143; Oxnard PD press release 2/27/26; Ventura County Sheriff audit; San Francisco class action (Gibbs Mura, filed 2/26/26); Richmond CA contract renegotiation; Costa Mesa OC DA guilty plea; AB 481 (Govt. Code 36045); EFF Atlas of Surveillance; CalMatters ALPR investigation.