

City of Alameda



Memorandum

Date: September 14, 2026
To: Gerry Beaudin, City Manager *EB*
From: Nishant Joshi, Chief of Police
For: Mayor and Councilmembers
Subject: **Automated License Plate Reader System & Data Protection**

1. Purpose

This memorandum provides an update on Automated License Plate Reader (ALPR) data and its potential misuse. It summarizes the City of Alameda Police Department's (APD) independent review of the City's Flock Safety network, the corrective actions Flock Safety has since implemented, the safeguards APD already had in place, and the legal framework (both constitutional and statutory) that governs this technology.

2. Background

APD uses Flock Safety fixed ALPR cameras to photograph license plates and vehicle characteristics (type, color) on public roadways. The system does not use facial recognition and does not capture video or audio. Captured data (plate number, vehicle description, date/time, and camera location) is used to generate investigative leads tied to stolen-vehicle reports, missing-persons cases, and active investigations. A trained officer reviews and verifies every alert before any enforcement action is taken. ALPR data is never the sole basis for a stop, citation, or arrest.

This technology is not surveillance in the way that term is commonly understood. Surveillance typically refers to ongoing, targeted observation of a specific person over time, including following where a particular individual goes, whom they meet, or what they do. ALPR cameras do not do this. The system does not track or follow any individual; each camera passively records the license plates of vehicles passing a fixed location at a given moment, regardless of who is inside. A search returns whether a specific plate has appeared at a fixed camera location. It does not allow an officer to watch, follow, or monitor a person's movements in real time.

2.1 Grounding in 21st Century Policing's Technology Pillar

The 2015 President's Task Force on 21st Century Policing organized its recommendations into six pillars, one of which (Pillar Three: Technology and Social Media) addresses how agencies should adopt tools such as ALPR. APD's program reflects several of that pillar's core recommendations:

- Recommendation 3.1.2 states that technology's impact on privacy should be addressed consistent with the protections provided by constitutional law. APD's Fourth Amendment analysis (Section 5.1 of this memo) and its access, retention, and audit controls (Section 4.3 of this memo) are built around that standard.
- Recommendation 3.2.1 calls on agencies to encourage public engagement when developing policy for new technology. APD's ALPR policy was developed and adopted through public City Council hearings before deployment, consistent with this recommendation.
- Recommendation 3.2.2 calls for an evaluation or assessment process to gauge a new technology's effectiveness. APD's regular internal audits of search activity (Section 4.3 of this memo) serve this function.
- Recommendation 3.3 calls on the U.S. Department of Justice to develop best practices governing the acquisition, use, retention, and dissemination of auditory, visual, and biometric data by law enforcement. California's own statutory framework for ALPR data (Civil Code § 1798.90.5 et seq., discussed in Section 5.2 of this memo) reflects the same principle, and APD's policy of not sharing its network with any outside agency goes beyond it.
- Recommendation 3.5 calls on agencies to adopt best practices for technology-based community engagement that increases community trust and access. This memo and the accompanying public fact sheet (Attachment A) are intended to serve that purpose.

3. National Concerns and APD's Review

Recent reporting has centered on two concerns nationally: (1) unauthorized cross-agency access to ALPR networks, and (2) the potential use of ALPR data for civil immigration enforcement. In response, APD conducted an internal audit of its network access history and met with Flock Safety leadership (in person and virtually, on multiple occasions) to fully understand the scope of any historical vulnerabilities and confirm what corrective actions have been taken.

4. Findings

4.1 Historical Network Vulnerability (2023–2024)

In 2023, a design flaw in Flock's administrative system enabled an ALPR administrator in one state to change their listed location to California and, using a full license plate number, query California ALPR networks (including Alameda's) for a match. A partial plate was insufficient for this; the requester needed the full license plate number.

APD's review of its historical network audit logs found the following:

- Alameda's network was queried ("pinged") by out-of-state administrators 36 times over 12 months, from March 2023 to March 2024.
- These queries were part of a pattern affecting all California ALPR networks (more than 3,100 agencies) and were not targeted specifically at Alameda.
- None of the 36 queries were coded with an immigration-enforcement search reason.
- Flock does not retain search history beyond 30–60 days, so APD cannot retroactively confirm with certainty whether any of the 36 queries received a data response from Alameda's network. Based on the system's mechanics and the volume of networks queried, APD's analysis estimates that the probability that any of the 36 queries returned data from Alameda specifically is approximately 0.0003%. This is an estimate, not a confirmed finding, and is presented here in the interest of full transparency.

This vulnerability occurred during APD's initial adoption of ALPR technology and was not the result of any action or inaction by APD; it stemmed from the design of Flock's national administrative system.

4.2 Corrective Action Taken by Flock Safety

Flock Safety has acknowledged this vulnerability and implemented the following corrective measures:

1. Disabled the ability for out-of-state administrators to access any California agency's network.
2. Blocked all California agencies from sharing data with out-of-state and federal agencies.
3. Implemented automatic blocking of searches associated with immigration-enforcement or reproductive-health keywords.
4. Blocked federal agencies from being able to identify which California agencies use Flock Safety.
5. Blocked data sharing between California agencies and federal agencies.
6. These blocks have been in place since 2025, and Flock's system can now identify which agency initiated any given query.

4.3 Safeguards Already in Place at APD

Independent of Flock's system-wide corrective action, APD has maintained the following practices throughout its use of this technology:

- Network access and data sharing are two different things, and APD's policy treats them differently. Outside agencies can never access APD's live ALPR network directly; no external agency can log in and run their own searches against Alameda's cameras. To date, APD has received approximately 200 written requests from other agencies for this kind of network access, and all 200 have been denied.

- Separately, APD may share legally obtained and retained case-specific ALPR data (not network access) with another agency when that agency submits a formal written request establishing a legitimate law enforcement purpose, and the request is reviewed and approved by a designated commander, consistent with APD Policy 462 and California law. Federal immigration agencies (ICE and CBP) are categorically excluded from this process; APD does not share ALPR data for immigration enforcement under any circumstances. APD reports the number of agencies that received data through this process in its annual public ALPR usage report to City Council, consistent with the transparency principle discussed in Section 2.1.
- By default, APD's search tool returns results only from Alameda-owned cameras. An APD officer may expand a search to include other agencies' cameras if those agencies make them available to APD. The reverse is not true. Meaning other agencies cannot add Alameda's cameras to their own searches or otherwise access Alameda's data held by Flock.
- Camera locations are visible only to agencies within a 50-mile radius, and visibility does not equal access: agencies within this radius can only see that APD has cameras and the locations of those cameras. Agencies beyond 50 miles, and all federal agencies, currently cannot see that APD operates ALPR cameras at all.
- A full, confirmed license plate is required before any cross-network "lookup" can occur; the "search" function (partial plate, vehicle description) used day-to-day does not expose APD's network to outside queries. As of 2025, statewide lookup is available to all California agencies if they opt in, but nationwide lookup is not. As to the statewide lookup, APD has opted out.
- APD conducts regular internal audits of its officers' search activity to confirm compliance with department policy and authorized use.
- No search of APD's system has been coded with immigration enforcement as its stated purpose.

4.4 Flock Safety's Public Privacy Commitments

In addition to the corrective action and internal audit described above, Flock Safety's public Trust Center (flocksafety.com/trust) documents company-wide policy commitments and practices that reinforce APD's own practices. These commitments and practices are summarized below:

- Data access and permissions are set by the local agency, not by Flock; permissions are role-based, and every search is tied to a specific user and logged automatically. There is no open browsing or anonymous searching of the system.
- There is no national database of ALPR data. Each agency controls its own data independently; sharing with other agencies happens only if that agency opts in, and nothing is shared automatically.
- Flock states its system is built to support specific, case-based investigations and is not designed for broad, continuous monitoring of individuals.

- Flock has publicly stated it does not work with, and is not owned by, Palantir, and that Palantir does not have access to Flock customer data, addressing a recurring public misconception.

These public commitments and practices are consistent with and support the assurance APD received directly from Flock Safety leadership that no APD data is shared outside APD without APD's authorization.

4.5 Context: ALPR Compared to Other Law Enforcement Databases

Officers already have lawful, routine access to databases containing far more sensitive information than ALPR collects, through the California Law Enforcement Telecommunications System (CLETS), which connects to FBI and California DMV databases. Unlike ALPR, which is limited to a plate number, vehicle description, date/time, and location, CLETS-connected systems can return a person's full criminal history, active wants and warrants, restraining and protective orders, DMV driver's license photo and home address, and vehicle registration details. Unlike ALPR data, which is automatically purged within 30 days for non-hit detections (Section 5.2), the criminal history, warrant, and DMV records available through CLETS are retained indefinitely and are not subject to automatic deletion.

Access to these systems already carries a stricter accountability regime than ALPR does. Misuse of CLETS is not merely a policy violation; it is a crime.¹ Accessing CLETS outside the scope of an officer's official duties violates Penal Code § 502, and Government Code § 6200, both of which carry felony penalties, and misuse of criminal history information carries separate penalties under Penal Code §§ 11141–11143 and 13302–13304, and Vehicle Code § 1808.45 for DMV information specifically. The California Department of Justice audits CLETS access, and agencies are required to report confirmed misuse annually or risk losing CLETS access altogether.

This context is relevant for two reasons. First, it shows that officers already have lawful access to tools that, if misused, would be far more invasive than ALPR, and that the profession already operates within (and is held accountable to) an established framework of criminal, civil, and administrative consequences for misuse. Second, it means the safeguards described in Section 4.3 (the case-number requirement, network restrictions, and independent audits) are consistent with and, in some respects, exceed the accountability standards that already govern far more sensitive systems in daily law-enforcement use.

5. Legal Framework

Two distinct bodies of law govern this technology, and public discussion often conflates them. Both are relevant to APD's program, but they answer different questions.

5.1 Fourth Amendment: Does ALPR use require a warrant?

¹ Although APD is not currently aware of any criminal prosecutions for misuse of Flock/ALPR data, according to the City Attorney's Office, Penal Code § 502 likely applies to the unlawful access or misuse of ALPR data.

No U.S. Supreme Court decision has directly addressed ALPR. However, state and federal courts (at the trial and appellate levels) have consistently held that photographing a license plate on a public roadway does not constitute a Fourth Amendment “search,” because there is no reasonable expectation of privacy in a plate already exposed to public view. Lower courts primarily have relied on the following Supreme Court opinions:

- *United States v. Knotts*, 460 U.S. 276 (1983) (holding that “A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”)
- *United States v. Jones*, 565 U.S. 400 (2012) (holding that physically attaching a GPS tracker to a vehicle is a search under the Fourth Amendment). This holding is distinguishable from ALPR and *Knotts* because in *Knotts*, the beeper was added to a container before it came into the driver’s possession, and with ALPR, nothing is attached to the vehicle and captures are discrete rather than continuous.
- *Carpenter v. United States*, 585 U.S. 296 (2018) (holding that “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through cell-site location information” and therefore a warrant is required to access such information). The Court specifically noted in dicta that “we do not . . . call into question conventional surveillance techniques and tools, such as security cameras.”

Lower courts² have analyzed the question of whether the Fourth Amendment applies to ALPR data:

- *Commonwealth v. McCarthy*, 484 Mass. 493 (2020): The Massachusetts Supreme Court held that the use of four ALPR cameras at fixed locations did not constitute a search under the Fourth Amendment. The court noted that “this limited surveillance does not allow the Commonwealth to monitor the whole of the defendant’s public movements, or even his progress on a single journey.”
- *United States v. Yang*, 958 F.3d 851 (9th Cir. 2020): Although the Ninth Circuit panel’s majority opinion in *Yang* declined to address whether use of ALPR violated Yang’s Fourth Amendment rights, Judge Carlos T. Bea wrote in a non-binding concurrence that he would have affirmed the lower court “on the grounds that the search of the LEARN database did not require a warrant because the information in the database did not reveal ‘the whole of [Yang’s] physical movements,’ and therefore did not infringe on that reasonable expectation of privacy.” (quoting *Carpenter*, 585 U.S. at 313).
- *Schmidt v. City of Norfolk*, 819 F.Supp.3d 492, 510-13 (E.D. Va. Jan. 27, 2026): A federal district court judge ruled, as part of his order on a summary judgment

² Although the issue of ALPR and the Fourth Amendment has been briefed in at least one case in the California Court of Appeals by amicus curiae Electronic Frontier Foundation and the ACLU, *People v. Gonzalez* (2019) 42 Cal.App.5th 1144, the court did not reach or rule on this issue in that case and APD is not aware of other state appellate rulings on constitutional limitations on the use of ALPR.

motion, that “even in the aggregate, the ALPR cameras do not approach the near-constant surveillance of cell-phone users’ public and private movements that so concerned the Supreme Court in *Carpenter*,” and therefore, “Plaintiffs were not subject to an unconstitutional search.” The court noted in its factual findings that “the limited number of photographs available on a 21-day rolling basis from 75 camera clusters in Norfolk does not “track” the whole of a person’s movements nor does it provide an “intimate” window into where citizens drive, park, visit, linger, sleep, or patronize.”

- *State v. Simonson*, 36 Wash.App.2d 1041, 2026 WL 242157 (Wash. Ct. App. Jan. 29, 2026): The Washington State Court of Appeals, Division 3, held that “The Flock ALPR system’s photograph of the vehicle Simonson was operating in plain view on a public road did not disturb his private affairs under article 1, section 7 of the Washington Constitution.” (Generally, the Washington State constitution’s privacy protections are more extensive than those provided under the Fourth Amendment. See *State v. Alexander*, 10 Wash.App.2d 682, 687 (2019).)

5.2 Data Privacy Protections Imposed by the California Legislature

This is a separate legal question from the Fourth Amendment analysis above, and the two should not be conflated. Even though courts have found that reading a plate is not a constitutional “search,” California law separately defines and regulates ALPR data. Under California Civil Code § 1798.90.5 et seq. (enacted via SB 34), any public agency operating ALPR must:

- Maintain reasonable security safeguards (operational, administrative, technical, and physical) to protect ALPR data from unauthorized access, destruction, use, modification, or disclosure (Civ. Code § 1798.90.51(a)).
 - ✓ **APD complies:** Access to ALPR data is role-based, every search is logged and independently audited, and camera data is encrypted in transit and in storage (Section 4.3, supra).
- Adopt and publicly post a written usage and privacy policy governing the collection, use, maintenance, sharing, and dissemination of ALPR data (Civ. Code § 1798.90.51(a)(b)(1)).
 - ✓ **APD complies:** Policy 462 is APD’s adopted, written ALPR usage and privacy policy, publicly available on APD’s transparency portal (<https://transparency.flocksafety.com/alameda-ca-pd>).
- Refrain from selling, sharing, or transferring ALPR data to anyone other than another public state agency, and only as otherwise permitted by law (Civ. Code § 1798.90.55(b)).
 - ✓ **APD complies:** APD’s network is never shared, and case-specific data is disclosed only through the formal written-request-and-commander-approval process described in Section 4.3; APD does not sell ALPR data under any circumstances.

APD's practice of not sharing its network with any outside agency (public or private) exceeds this statutory floor. The law permits sharing with other public state agencies, and APD chooses not to do so.

Notwithstanding these statutory protections, APD must also balance privacy concerns with other state law, namely, the California Public Records Act. In *ACLU Foundation of Southern California v. Superior Court*, 3 Cal.5th 1032 (2017), the California Supreme Court held the following:

- The public interest in preventing the disclosure of *unaltered* license plate scan data would “jeopardize the privacy of everyone associated with a scanned plate,” and therefore “clearly outweighs the public interest served by disclosure of these records.” *Id.* at 1044.
- However, the trial court erred in concluding that the disclosure of even bulk anonymized or redacted plate scan data would frustrate law enforcement efforts, and remanded the case for the trial court to undertake a new balancing analysis with appropriate consideration of various methods of anonymization. *Id.* at 1045-46. In other words, the California Supreme Court *did not explicitly forbid* the disclosure of bulk ALPR data to any person who might request it. The implication is that this would be evaluated on a case-by-case basis.

In practice, this framework interacts directly with APD's 30-day retention limit. The Public Records Act governs the disclosure of existing records; it does not itself dictate how long an agency must keep them. Retention is instead controlled separately, by APD's own written retention schedule adopted pursuant to Civil Code § 1798.90.5 et seq. Because APD automatically deletes non-hit ALPR detections after 30 days, a records request for that underlying photo data made after the 30-day window will return no responsive records. This is not because of a claimed exemption, but because the data no longer exists under a routine, pre-existing schedule.

Within the 30-day window, however, there currently is no categorical protection for “anonymized” bulk data. Rather, APD staff will have to consider any requests for such data based on the circumstances of each request and the data being requested.

This analysis also changes if the ALPR data becomes evidence and therefore part of a specific case. Confirmed hotlist matches tied to an actual case may be retained for the life of that case and separately assessed under the law-enforcement investigatory-records exemption (Gov. Code § 7923.600(a)).

APD's search audit logs and its annual public ALPR usage report to the City Council are maintained under separate administrative retention schedules beyond the 30-day window. These logs and the annual public ALPR report do not contain any license plate information. The annual report is already public, and requests for search audit logs would be evaluated under applicable law by APD staff.

In short, current applicable case law would find APD's use of ALPR without a warrant to be constitutional. At the same time, California state law independently requires strict controls over how that data is secured and shared once collected, and APD's current policies and practices exceed these requirements.

6. Conclusion

The vulnerability identified in the national reporting was a system-wide design issue affecting all California Flock networks, not a gap specific to Alameda's program or a result of any APD policy failure. APD's audit found no evidence that Alameda data was used for immigration enforcement and found only a statistically minimal chance that any of the 36 historical out-of-state queries received data from Alameda's network. Flock Safety has since implemented corrective action closing this vulnerability, and APD's own access-control, audit, and non-sharing practices (already in place before this issue surfaced) continue to exceed both Flock's default configuration and California's statutory requirements.

APD is not opposed to evaluating other vendors when its current agreement with Flock Safety expires, and the department expects to consider a competitive process at that time, consistent with the City's standard procurement practices. Currently, however, APD is under an active contract with Flock Safety, and the company has demonstrated alignment with the department's expectations for privacy, security, and accountability throughout the term of that agreement. Should Flock Safety violate the terms of that agreement, including its privacy and data-sharing commitments, such a violation would constitute grounds for early termination of the contract. Based on Flock Safety's performance and compliance to date, and subject to the ongoing audit and legal monitoring described above, APD is comfortable continuing with Flock Safety as its ALPR vendor for the remainder of the current contract term.

A public-facing fact sheet summarizing this technology and APD's safeguards is attached for reference and community distribution. Attachment B provides a basic illustration of how the technology works. Additionally, APD provides a public-facing transparency portal on its website regarding the FLOCK Safety ALPR program.

Sources

- Alameda Police Department Policy Manual, Policy 462 — Automated License Plate Readers (ALPR).
- Final Report of the President's Task Force on 21st Century Policing (May 2015), Pillar Three: Technology and Social Media, Recommendations 3.1–3.5.
- Flock Safety, "Privacy, Data & Civil Liberties Policies," flocksafety.com/trust (accessed August 31, 2026).

Attachment A – FLOCK ALPR Fact Sheet "Flock Safety License Plate Reader Cameras: What Alameda Residents Should Know"

Attachment B – FLOCK ALPR Illustrated Guide

cc: Len Aslanian, Acting City Attorney
Leigh Grossman, Police Auditor
Lara Weisiger, City Clerk
Department Heads

FLOCK SAFETY LICENSE PLATE READER CAMERAS

What Alameda Residents Should Know

APD uses Flock Safety automated license plate reader (ALPR) cameras as one tool to help solve crimes, recover stolen vehicles, and locate missing people. We know residents have real questions about privacy — this sheet explains how the technology works and the safeguards APD has put in place, several of which go beyond Flock's own recommendations and what many other agencies require.

WHAT THE TECHNOLOGY DOES

- Fixed cameras photograph license plates, vehicle type, and color as vehicles pass on public roads.
- Captures plate number, vehicle description, date/time, and camera location only.
- No facial recognition — the system cannot identify people, only vehicles.
- No live video and no audio recording.

HOW APD USES IT

- Alerts officers to vehicles tied to stolen-vehicle reports, missing persons, and active investigations.
- Provides an investigative lead only — never the sole basis for an arrest or citation.
- A trained officer always reviews and verifies an alert before taking action.
- Used for serious public-safety purposes, not routine traffic enforcement.

PRIVACY SAFEGUARDS — APD POLICY

- Data not tied to a case is automatically deleted after 30 days at most; data tied to an active case may be retained until the case closes.
- APD's network itself is never opened to another agency. Specific data may be shared only when another agency submits a formal written request with a legitimate law-enforcement purpose, approved by a commander; federal immigration agencies are never eligible for this process.
- Never used for civil immigration enforcement.
- Access limited to trained, authorized personnel based on job role.

ACCOUNTABILITY & OVERSIGHT

- Every search requires a documented case number and a legitimate law-enforcement purpose.
- All searches are logged and independently audited to detect misuse.
- Confirmed misuse results in immediate access suspension and disciplinary review.
- Built on 21st Century Policing principles: transparency, accountability, and community trust.

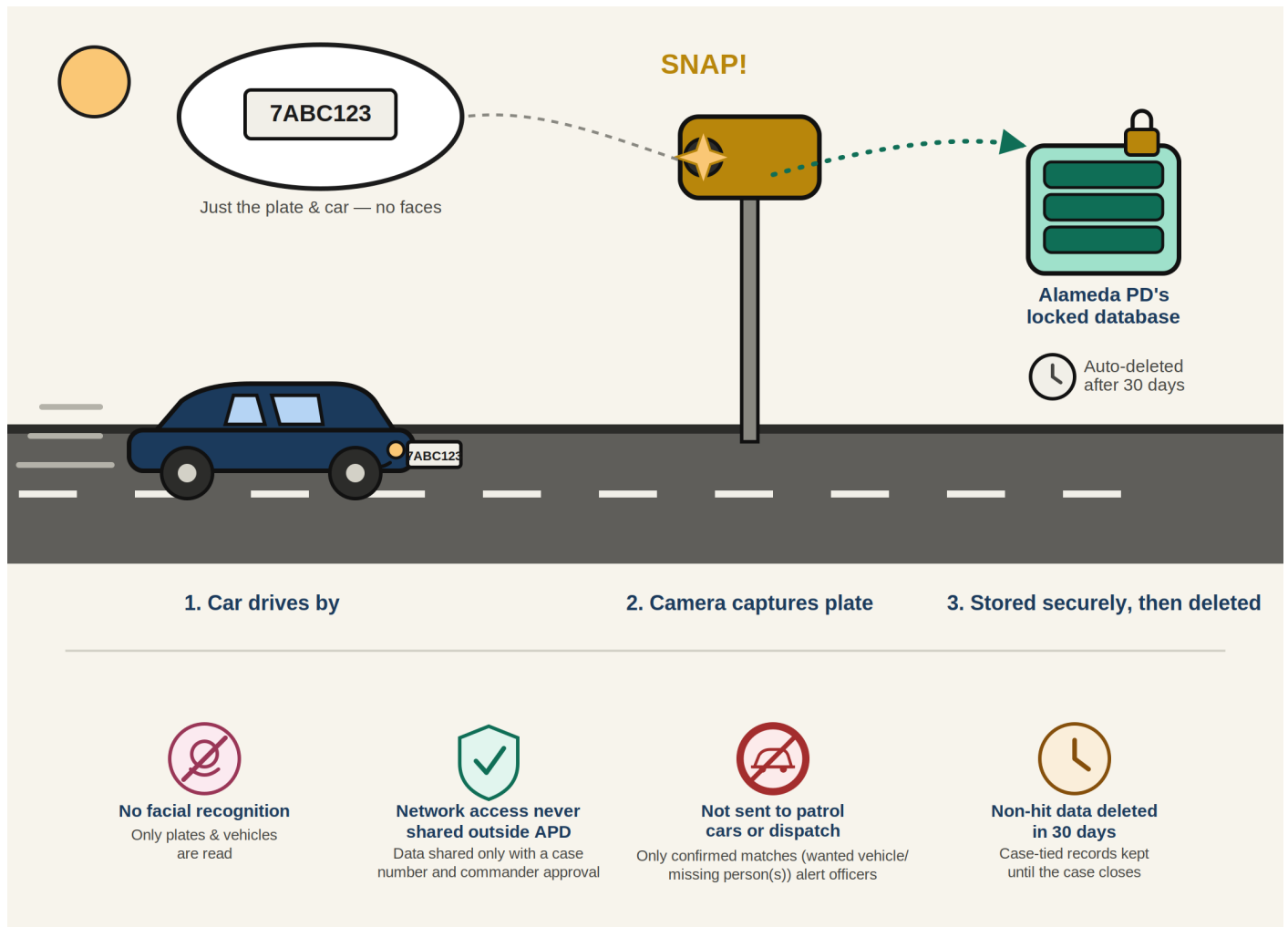
FREQUENTLY ASKED QUESTIONS

- Does this use facial recognition? No. The system cannot identify people — only vehicles.
- Can immigration authorities access this data? No. APD's ALPR data is never used for civil immigration enforcement, and no outside agency — federal or otherwise — can access APD's network.
- Is my data shared outside Alameda? APD's network is never shared or opened to another agency. Specific data may be shared, but only after a formal written request and commander approval — and never with federal immigration agencies.
- What's the legal basis for this program? Courts have consistently held that photographing a plate on a public road isn't a Fourth Amendment search; separately, California Civil Code § 1798.90.5 sets strict security, retention, and no-sale requirements APD's policy meets or exceeds.

Questions or concerns? We want to hear them. Contact the Alameda Police Department at 510-337-8340 or visit <https://www.alamedaca.gov/Departments/Police-Department> to view our policies, the FLOCK transparency portal, or FLOCK Cameras FAQs.

HOW THE LICENSE PLATE CAMERA WORKS

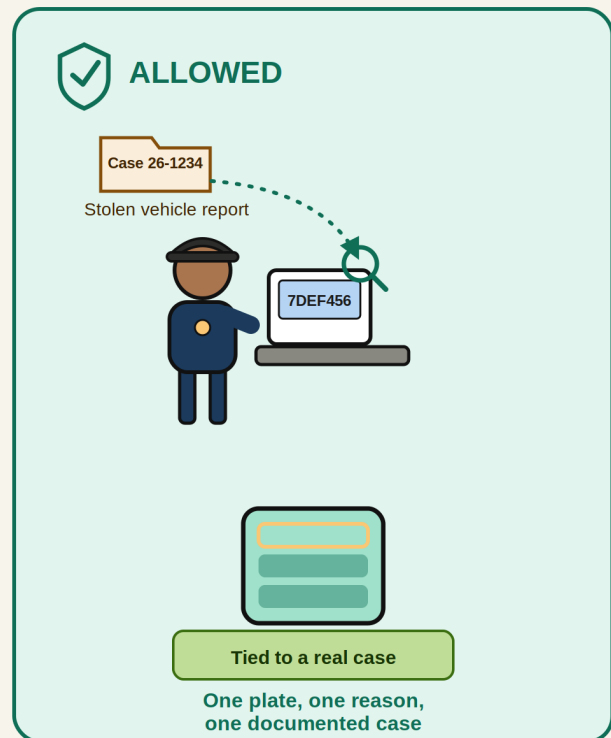
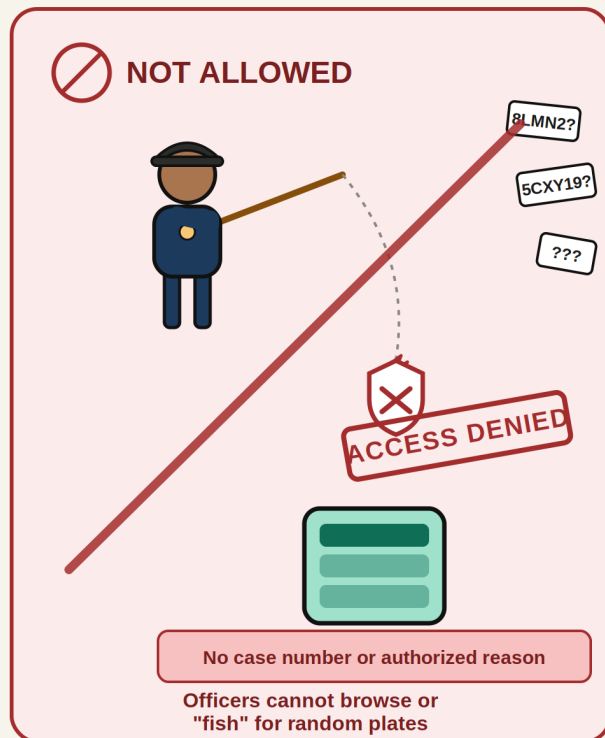
A simple, illustrated look at what happens in three steps



That's it — no facial recognition, no live video, and the photo doesn't stay forever. For the full details on privacy protections and oversight, see the accompanying fact sheet.

WHAT OFFICERS CANNOT DO

There's no fishing in the database — every search needs a reason



Case number required
Every search needs one



No curiosity searches
Personal lookups are banned



Logged & audited
Every search is reviewed

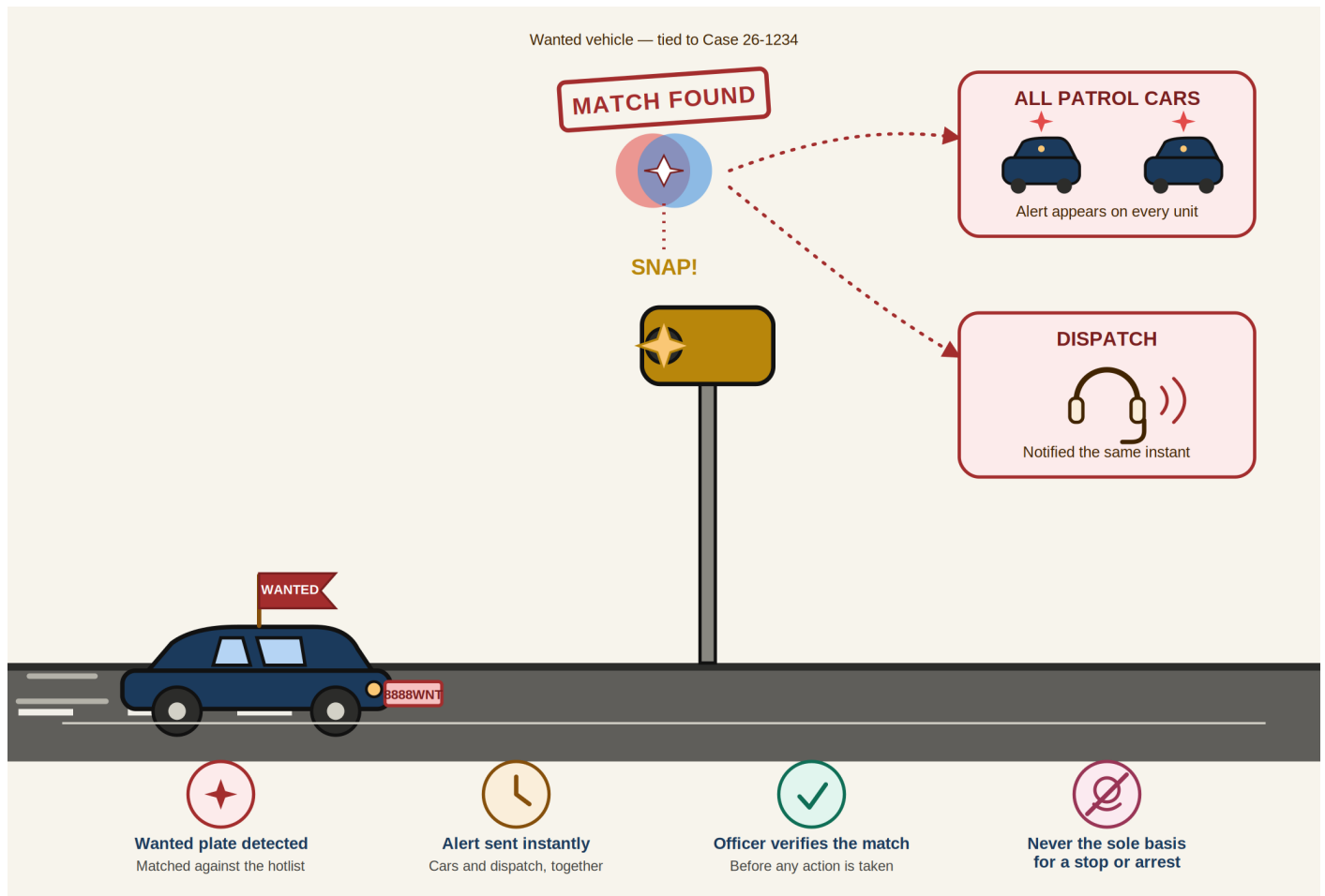


Violations mean lost access & discipline

No case number, no search — period. Every lookup is tied to a specific investigation and reviewed afterward.

WHEN A WANTED PLATE IS FOUND

A confirmed match alerts patrol cars and dispatch instantly



A real match reaches every unit and dispatch at once. An officer still verifies the match before any stop or arrest is made.