The City of San Diego

M E M O R A N D U M

DATE: June 13, 2025

TO: Tim Blood, Chair, Privacy Advisory Board

FROM: Kris McAndrew, Lieutenant, Watch Commander

SUBJECT: Update on Automatic License Plate Reader (ALPR) Use Policy and Audit Improvements

---

This memo serves as an update on two areas the Privacy Advisory Board (Board) asked the San Diego Police Department (Department) to explore: strengthening the ALPR Use Policy to better align with Senate Bill 34 (SB 34) and enhancing auditing practices related to surveillance technologies.

1. ALPR Use Policy Enhancements

At the Board's recommendation, the Department reviewed the ALPR Use Policy with the goal of aligning more clearly with SB 34. In partnership with the California Department of Justice, SDPD is working to revise the policy to better reflect the very limited and clearly defined circumstances under which ALPR data may be shared.

As part of this review process, the Department discussed a handful of instances in which ALPR data was shared with federal and out-of-state law enforcement agencies for non-immigration related criminal cases. Importantly, these agencies never had direct access to the Department's ALPR database. Upon further review of SB 34, the Department ceased all such data sharing for any reason. That directive was immediately communicated to the Department's internal teams in April and formally reinforced in a Department-wide order issued on May 23, 2025 (See Exhibit A).

Additionally, the Department plans to revise the ALPR Use Policy to better clarify responsibilities as an end user when other law enforcement agencies or organizations choose to voluntarily share their ALPR data with SDPD.

The Department expects to bring a revised ALPR Use Policy to the Board in the coming weeks for review and input.

2. Audit Process Improvements

The Board also encouraged the Department to enhance auditing processes for surveillance technologies. This year marked the first time any City department conducted a

comprehensive audit and review under the TRUST Ordinance. While there were both successes and lessons learned, the Department is currently assessing its procedures and has already identified several areas for improvement.

One important issue came to light in response to a recent California Public Records Act request. The Department discovered a two-week period at the beginning of the ALPR system's launch that had been accidentally omitted from the Annual Report submitted to the Board on Feb. 1, 2025.

The agreement for situational awareness cameras (commonly known as Smart Streetlights) and ALPR devices states the Department does not provide other agencies access to the Department's ALPR Flock database. However, when the ALPR system was launched, the appropriate setting was not correctly implemented, which allowed other State law enforcement agencies to run searches against the Department's ALPR database. As a result, from December 29, 2023, to January 17, 2024,* the Department's ALPR camera system was included in 12,914 searches conducted by other California law enforcement agencies across Flock's network, the subcontractor providing the Department's ALPR equipment and services.

A detailed breakdown of ALPR search activity during the specified timeframe is provided in an accompanying data summary (see Exhibit B).

The Department discovered the issue through an internal audit on or about Jan. 17, 2024. The Department immediately notified Flock of the error, and Flock at once corrected the data sharing settings. It has not occurred since. However, this initial two-week period was mistakenly left out of the Department's ALPR Annual Report. The Department will be resubmitting its Annual Report to include these searches.

Additionally, moving forward, the Department's audit process will include multiple layers of oversight to prevent such omissions. This improved structure will ensure more accurate, transparent, and comprehensive reporting in the future. The Department has also taken steps to improve internal education on its responsibilities under the TRUST Ordinance, including issuing a Department-wide directive on April 25, 2025 (see Exhibit C).

Finally, while the ALPR Annual Report noted that data was shared with federal investigators in non-immigration-related criminal cases, it is important to emphasize that none of the unintended access to the Department's ALPR system from December 29, 2023, to January 17, 2024, involved federal or out-of-state law enforcement agencies.

The Department appreciates the continued engagement and thoughtful feedback from the Board and will keep the Board informed as progress is made on these two key initiatives. The Department looks forward to sharing more detailed updates soon.

- *An additional 795 search attempts occurred on Dec. 27, but no cameras were turned on at that time.*

Exhibit A: OR 25-19 – Sharing of Automated License Plate Recognition Data Per SB 34

SAN DIEGO POLICE DEPARTMENT
ORDER

DATE/TIME: MAY 23, 2025 1900 HOURS

NUMBER: OR 25-19

SUBJECT: SHARING OF AUTOMATED LICENSE PLATE RECOGNITION DATA PER SB34

SCOPE: ALL MEMBERS OF THE DEPARTMENT

DEPARTMENT PROCEDURE AFFECTED: 1.51

Over the last year, Automated License Plate Recognition (ALPR) technology has proven to be a valuable tool in investigating and quickly apprehending subjects wanted in connection with crimes throughout San Diego. While this technology is available to approved Department Members, per Senate Bill 34, California Law Enforcement agencies are not allowed to share any ALPR data with private entities, out-of-state law enforcement agencies, or federal agencies.

Effective immediately, all Department Members who have access to ALPR data shall not share any ALPR information with private entities or out-of-state or federal agencies, including out-of-state and federal law enforcement agencies.

For a summary of SB34 from the California Department of Justice, please click on the link below.

2023-DLE-06: California Automated License Plate Reader Data Guidance

If you have any questions, please contact Lieutenant K. McAndrew at kmcandrew@pd.sandiego.gov

---

Please read at squad conferences and give a copy to all personnel.

Exhibit B: Breakdown of ALPR Search Activity from Dec. 28, 2023 to Jan. 17, 2024

Date	Active Cameras	Searches
28-Dec	0	795
29-Dec	7	1099
30-Dec	7	462
31-Dec	7	717
1-Jan	7	231
2-Jan	7	592
3-Jan	9	1060
4-Jan	10	1040
5-Jan	13	655
6-Jan	13	554
7-Jan	13	343
8-Jan	21	571
9-Jan	26	922
10-Jan	32	981
11-Jan	35	898
12-Jan	35	514
13-Jan	35	458
14-Jan	35	200
15-Jan	35	379
16-Jan	39	635
17-Jan	41	503

2023 Searches	3,073
2024 Searches	10,536
Total	13,609
December 28, 2023, Searches	-795
Actual Searches	12,914

Exhibit C: OR 25-13 – Audits & Inspections of Surveillance Technologies

SAN DIEGO POLICE DEPARTMENT
ORDER

DATE/TIME: APRIL 25, 2025 1000 HOURS

NUMBER: OR 25-13

SUBJECT: AUDITS & INSPECTIONS OF SURVEILLANCE TECHNOLOGIES

SCOPE: ALL MEMBERS OF THE DEPARTMENT

DEPARTMENT PROCEDURE AFFECTED: SDPD INSPECTION MANUAL

To better govern the responsible utilization of the San Diego Police Department's approved technologies which fall under the City of San Diego's Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance, the units that manage the specific surveillance technology will audit/inspect them on at least a quarterly basis.

To prepare for the required Annual Report each year, as set forth in SDMC 210.0108, the managing unit (The managing unit is the person(s) recognized as the Subject Matter Expert (SME) for the TRUST Ordinance reporting or who controls the equipment) shall continually track and document the following types of information, as listed in SDMC 210.0102:

1. **Quantity of data:** A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the surveillance technology.

2. **Name of the Recipient of Data, Legal Standards, etc.:** Whether and how often data acquired through the use of the surveillance technology was shared with any non-City entities (e.g. District Attorney or other Law Enforcement Agencies), the name of any recipient entity, the types of data disclosed (e.g. Body Worn Camera footage, drone footage, data reports, etc.), under what legal standards the information was disclosed (e.g. warrant, criminal discovery process, etc.), and the justification for the disclosure, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

3. **Physical Deployment:** A description of the physical objects to which the surveillance technology hardware was installed, if applicable, and without revealing the specific location of the hardware, and a breakdown of the data sources applied or related to the surveillance technology software.

4. **Software updates, hardware upgrades, reasoning for the change:** A list of the software updates, hardware upgrades, and system configuration changes that expanded or reduced the surveillance technology capabilities, as well as a description of the reason for the changes, except that no confidential or sensitive information should be disclosed that

would violate any applicable law or undermine the legitimate security interests of the City.

4. **Where the tech was deployed geographically:** A description of where the surveillance technology was deployed geographically, by each City Council District or police area, in the applicable year.

5. **Community Complaints or Concerns:** A summary of any community complaints or concerns about the surveillance technology and an analysis of its Surveillance Use Policy, including whether it is adequate in protecting civil rights and civil liberties, and whether, and to what extent, the use of the surveillance technology disproportionately impacts certain groups or individuals.

5. **Data breaches or Improper Use:** Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

6. **Crime Statistics:** Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes. (<u>This includes any success stories of the use of the technology.</u>)

7. **CPRAs:** Statistics and information about California Public Records Act requests regarding the specific surveillance technology, including response rates, such as the number of California Public Records Act requests on the surveillance technology and the open and close date for each of these California Public Records Act requests.

8. **Cost:** Total annual costs for the surveillance technology, including any specific personnel-related and other ongoing costs, and what source will fund the surveillance technology in the coming year.

Effective immediately, the managing unit will conduct, at least, quarterly audits/inspections, which will include:

1. Selecting a minimum of 10 different uses of the technology, if applicable, within the timeframe, to confirm that protocols are being followed by department members who have access to surveillance equipment or software, following the criteria set forth in the technology's approved Use Policy.

    a. If the surveillance technology was used less than 10 times in the audit period, all uses shall be audited.

2. All managing units shall maintain, to the extent possible, a log of what data is shared with non-City entities as referenced in the Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance. San Diego Municipal Code § 210.0102(a)(2) and (c).

For example, the District Attorney's Office or other Law Enforcement Agencies are considered non-City entities under the TRUST Ordinance. City entities include any Department or staff member within the City of San Diego, including the City Attorney's Office, San Diego Fire-Rescue, etc.

3. All managing units will also review their approved Use Policy and confirm adherence to the policy. If any activity is outside of the scope of the Use Policy, it shall be immediately addressed and annotated for potential modification of the Use Policy during the Annual Report.

Audit/Inspection Documentation:

At the beginning of the quarter (April, July, September, and January) the Research, Analysis, and Planning (RAP) Unit will send out an email to all identified SMEs/Managing Units. The email will contain an audit form to be completed by the SME/Managing Unit.

1. These audits shall be submitted by the 15th of the month following the audit period (April 15th, July 15th, October 15th, and January 15th).

Annual Inspections:

RAP will conduct an audit of the TRUST Ordinance technologies in combination with their annual Departmental audits, which will include:

1. Confirmation of the managing units' audits/inspections and data collection.

2. Conducting an independent audit/inspection on items, such as the equipment/software as well as their access and use, that have not previously been inspected by the managing unit's quarterly inspections.

These audits/inspections will be documented in the RAP Unit annual inspection memo that is presented to the Deputy Chief for review and approval.

These audits/inspections will be in addition to any unit inspections that are deemed necessary by the commanding officer of each unit or the Chief of Police.

Data Breaches:

If a Department member becomes aware of a data breach during business hours, they shall **immediately** notify the Information Technologies Unit to begin securing the breach and assessing the intrusion or compromise to the Department data. The Information Technology Unit will contact RAP and report the data breach, along with the steps being taken to stop the breach.

If the breach is detected after hours, the discovering Department member shall **immediately** notify the Help Desk at (619) 531-2228, who will notify the on-call Information Technology

member of the breach. The Information Technology Unit will notify RAP of the breach for documentation purposes.

Improper Use:

If a Department member becomes aware of improper use of an approved technology, they shall notify their supervisor. The supervisor shall notify the managing unit for the technology, who shall review the issue and determine the next course of action (e.g. training, disciplinary investigation, etc.). The RAP Unit shall be notified of the improper use of the technology by the managing unit, and what the next course of action will be.

If you have any questions, please contact the RAP Unit, D/Sgt Ted Collins at jtcollins@pd.sandiego.gov.

Please read at squad conferences and give a copy to all personnel.