Privacy Advisory Board

MEMORANDUM

November 5, 2025

To: The Hon. Council President LaCava and Members of the San Diego City Council

From: City of San Diego Privacy Advisory Board

RE: PAB Review and Recommendation of the San Diego Police Department's Revised **ALPR Surveillance Use Policy**

I. Recommendation

The Privacy Advisory Board (PAB) recommends that the City Council approve the revised Surveillance Use Policy for Automated License Plate Recognition technology ("ALPR") contingent on completion of the modifications detailed below.

II. Overview and General Comments

The PAB greatly appreciates the work done to improve the ALPR Surveillance Use Policy and recognizes the substantial improvements reflected in the draft submitted. In part the following modifications build on the work done to further tighten and clarify the Surveillance Use Policy. However, the four comments from the April 2025 recommendation report were not adequately addressed in the new proposed Use Policy. Therefore, we re-raise those four issues which are documented below.

From the PAB April 2025 Recommendation: The PAB specifically recommends the four immediate amendments to the ALPR use policy:

■ Data storage policy: After fourteen days, absent a warrant, data must be deleted.

■ Access policy: After twenty-four hours, ALPR data should only be accessible with a court-approved warrant. The only exception to the warrant requirement should be when the safety of an individual is directly at issue. In such instances, SDPD should document

the circumstances and post online within three days a description of the reasons a warrant was not sought.

■ Audit policies: Provide audit policies that require regular, in-depth audits of all users to ensure ALPR data is being appropriately accessed, credential sharing is not occurring, and each ALPR search is properly justified.

■ Sharing data: Prohibit data sharing with federal and out-of-state entities. This should include immigration and non-immigration-related uses.

Additionally, the areas that need substantial improvement concern vendor oversight and management. The SDPD plays only an oversight role regarding the ALPR system and management, including data management. Neither the SDPD nor the City operate or maintain the ALPR system and they do not collect or maintain the ALPR data, even though they are ultimately responsible for these functions. Instead, as is common with this type of system, the system is run by a third-party vendor, and the collected data is stored and managed by third-party vendors. The SDPD must specify its expectations of vendors and the respective roles and responsibilities played by each party, including delineating the SDPD's oversight and management using commercially reasonable and widely accepted methods for doing so.

The PAB also recognizes that the City's use and proper management of Surveillance Technologies and the data they generate is evolving and improving because of the TRUST Ordinance. The PAB encourages further work to achieve and help define best practices regarding Surveillance Technology, which is a goal the City can and should meet.

III. Issues to Address Concerning Proposed Surveillance Use Policy

The PAB requires the following matters to be addressed to obtain a recommendation for the adoption of the revised proposed ALPR Surveillance Use Policy.

The subheadings below correspond to the subheadings in the proposed Surveillance Use Policy.

Note that a section on "Data Access" must be added in compliance with the Trust Ordinance, SDMC §210.0102(q)(4). To increase clarity and ease of use, this section should be added even if the information required by the TRUST Ordinance is provided elsewhere in the Surveillance Use Policy and would repeat that information.

Likewise, the "Public Access" section should be moved to the seventh topic to correspond with the subsections in the TRUST Ordinance, SDMC §210.0102(q). This will promote clarity and ease of use.

Purpose

The PAB has no changes

Use

The first sentence should be deleted because it is not a description of the intended use of the technology. The first sentence to be deleted reads "ALPR systems have shown to be very effective tools in combating crime."

Additionally, the defined use is overly broad and open-ended. It states that ALPRs can be used for "Legitimate law enforcement purposes including, but are not limited to:" and lists examples. While examples are helpful, "legitimate law enforcement purposes" must be more precisely defined. Otherwise, ALPRs can be used in the future for purposes not contemplated or intended today.

For clarity, in the following sentence, "such as" must be replace with "including": "The Department will not integrate additional technologies, such as facial recognition or gunshot detection, into ALPRs." The use of "such as" leaves open the possibility that other technologies that are viewed as somehow different from the ones listed could be added without approval, which would violate the TRUST Ordinance.

In the paragraph delineated "(2)," replace "NCIC" with "National Crime Information Center ("NCIC")."

On the second page, fourth bullet point, replace "and" with "or" for clarity.

In the fifth bullet point, delete "indiscriminately" for clarity.

Data Collection

The PAB has no changes.

Data Protection

The Data Protection section does not accurately reflect how ALPR data is collected and maintained. The SDPD employs a vendor to operate the ALPR system, including collecting, storing, and managing data. The Use Policy must reflect this and set forth protocols to ensure the proper management and oversight of the ALPR system and its data.

The Use Policy must specify in detail the SDPD's vendor requirements for data protection. This includes vendor requirements, audit requirements, and the SDPD's oversight and vendor audit requirements. A program must be developed for the periodic review of any ALPR services provided by a third party. This must include a review of audit reports generated by the third party, such as SOC 2 Type 2 audit reports.

Finally, a provision must be added that in the event of a breach, unauthorized sharing, or other unauthorized disclosure, the people whose information was breached, shared, or otherwise disclosed must be notified within 30 days of when the SDPD becomes aware of the breach, unauthorized sharing, or unauthorized disclosure. Without such disclosure the provisions of SDMC §210.0109 (enforcement) are illusory.

Data Retention

Concerning the last paragraph, the details of the monthly audit must be specified, including actions to be taken when the audit reveals violations of the Use Policy or other abnormalities.

Third-Party Data Sharing

In the second paragraph, the following must be added to the sentence that reads "SDPD shall not:" so that the sentence reads "SDPD, or anyone acting on its behalf, including any vendor, shall not:"

In the last bullet point, change the sentence to add "or on behalf of" so the sentence reads: "Sell ALPR data obtained or received by or on behalf of SDPD."

Training

The PAB has no changes.

Auditing and Oversight

In the third paragraph, add the following at the end of the sentence that reads "The program administrator, who holds a supervisory rank, will conduct ALPR system audits" "no less than on a quarterly basis."

Public Access

The PAB has no changes.

Maintenance

While the ultimate responsibility for data and system security resides with the SDPD, the SDPD reasonably can have others perform the necessary tasks to meet this responsibility. However, the SDPD must clearly delineate the roles and responsibilities it and others are expected to perform and then have an audit system in place to ensure that all parties have performed those duties and any issues revealed are addressed. This includes delineation of roles and responsibilities between the SDPD and the City's IT Department and any vendors associated with ALPR technology and data.

The SDPD, or someone within the City acting on behalf of the SDPD, must know the vendor's protocols and periodically obtain verification of compliance with those protocols.

Only vendors willing to abide by these rules should be permitted to handle sensitive data, including the sensitive data collected by ALPR systems.

The Use Policy must specify the vendor's responsibilities and the City's responsibilities, including the SDPD's responsibilities.

The Use Policy should include a requirement that contractually requires the ALPR vendor to immediately notify the City whenever an unauthorized person or entity accesses any of the City's ALPR data. Further, the Use Policy should require that within 3 calendar days of receipt of a notification from an ALPR vendor that the City's data has been accessed by an unauthorized party, the City that receives the notification shall notify the chair of the Privacy Advisory Board and the City Council with the details of the received notification and any actions the City is taking as a result of the notification.