Privacy Advisory Board

MEMORANDUM

DATE: 17 April 2025

FROM: City of San Diego Privacy Advisory Board

TO: The Honorable Council President LaCava and Members of the San Diego City Council

RE: San Diego Police Department's 2025 Annual Surveillance Report

I. RECOMMENDATION

The Privacy Advisory Board (PAB) recommends that the City Council approve the report with modifications as indicated below.

II. OVERALL CONCERNS

The PAB has concerns in the oversight and compliance with the City of San Diego (City) policies and procedures in use of the various surveillance technologies. These core concerns include:

A. **Limited and Inconsistent Identification and Use of Key Performance Indicators (KPIs).** The usage and efficacy sections of the SDPD's Report (Report) contain only high-level metrics that are difficult to verify or track objectively.

B. **Lack of Proper Audit and Inspection Processes.** The Report states for most technologies that "[t]here were no reported violations of the Surveillance Use Policy or SDPD Policy or Procedure[.]" However, based on PAB's discussions with SDPD at PAB meetings, we believe these conclusions are not grounded in any rigorous and independent review of the technologies SDPD uses. Similarly, the Report states for most technologies that "SDPD has not received any complaints or concerns about these surveillance technologies and has not received any reports of disproportionate impacts." Again, however, strong community attendance at the PAB's March meeting indicates broad concern with SDPD's use of technologies that is apparently not being captured by the SDPD's current procedures.

C. **Lack of Clarity and Objective Procedures in Use of "Exigent Circumstances."** We note in several instances where technologies have been applied in locations or circumstances which were not directly related to the initial roll-out. In particular, some Smart Street Lights devices were moved to neighborhoods not originally included in the location plan based on "exigent circumstances." In these instances, however, no clear threats were noted or addressed.

III. POLICY-SPECIFIC RECOMMENDATIONS

A. KPIs: The SDPD needs to identify KPIs which are relevant, consistent and measurable for oversight and management of the particular surveillance technology. The PAB is open to working with SDPD to identify best practices regarding KPIs. Once we agree on the KPIs that are relevant, it is much more valuable to track. We request that SDPD identify and monitor at least one indicator for each of the four categories below and for each technology:

1. **Cost:** Total cost to buy, upgrade, and/or service.
2. **Usage:** Number of incidents in which technology was utilized.
3. **Results:** Number of arrests or prosecutions that resulted from each technology.
4. **Appropriate usage:** How many times did the department or a court deny the requested use of the given technology? Track each request, to include each usage and denial.

B. AUDIT & INSPECTION PROCESSES: The audit and inspection processes employed by SDPD for each technology lack meaningful scrutiny, do not have sufficient random checks, and fail to ensure that technologies are not being abused. The PAB believes a SDPD should create a detailed audit and inspection process for each technology. An audit/inspection program does not exist unless you have AT A MINIMUM:

- Clearly documented policies and procedures to be followed. Not general guidelines that personnel shall use when appropriate.
- Personnel doing the audit/inspection is independent of the personnel being inspected. This cannot be the supervisor, as noted in the SDPD practice.
- Formally planned inspection scope and sample size. A sample size will then be able to infer the accuracy of the overall population.
- Findings cannot be brushed aside as “one-offs” and explained away as not a problem. They must be extracted to the population and a legitimate effort at explaining their root causes must be made.
- Findings are tracked and analyzed regularly to identify trends and remediate their root causes.
- Personnel who have findings/exceptions from the policies must be held accountable.

C. EXIGENT CIRCUMSTANCES: The SDPD must establish policies and procedures when it is appropriate to adopt Exigent Circumstances. These policies and procedures must follow the definition of “exigent circumstances” discussed in San Diego City Ordinance Section 511.0101 and justification in Section 511.0104. When an Exigent Circumstances exception is invoked, notification should be made to the PAB within three business days.

IV. TECHNOLOGY-SPECIFIC RECOMMENDATIONS

Automated License Plate Recognition (ALPR) / Smart Streetlights

- We do not believe the three criteria of the TRUST Ordinance are being met by SDPD's widespread ability to use ALPRs to investigate any type of crime, including petty and non-violent crime.
- (1) the benefits to the community **do not** outweigh the costs;
    - SDPD conducted over 140,000 queries of the city's ALPR database during FY2024. According to SDPD's own accounting, ALPR technology provided usable information in 294 investigations. Put another way, only 00.2% of ALPR queries resulted in information that assisted in a successful investigation.
    - ALPR technology is a significant part of the Smart Streetlights program, on which $4.97 million from the City's General Fund has been spent during the past two fiscal years.
    - ALPR technology is expensive and being frequently queried by SDPD. However, the low number of investigations with any positive link to ALRP queries indicates this technology is more burdensome than beneficial.
- (2) civil rights and civil liberties are **not** being safeguarded;
    - The Surveillance Use Policy for ALPR permits SDPD to utilize the City's ALPR database for *any* crime. SDPD made clear in its meeting with the PAB that the Use Policy's authorization to use ALPR to "Locat[e] . . . vehicles subject to investigation" encompasses all vehicles under investigation in relation to any crime. The testifying officer admitted the Use Policy permits ALPR to be used to investigate non-violent petty crime, such as theft of a $10 grocery item.
    - All ALPR data is currently stored for thirty days and can be maintained indefinitely if investigators deem it to be evidence.
    - Neither the Use Policy nor Department Procedure 1.51 (referenced in the Use Policy) provides clear delineation of which users are authorized to use the ALPR database. SDPD can designate any sworn or non-sworn employee to access the database, and searches can be conducted without prior specific authorization for the incident or vehicle being investigated.
    - SDPD's ALPR data sharing practices conflict with the California Department of Justice's guidance on SB 34 (2015). In October, 2023, the California Department of Justice informed local law-enforcement agencies that "SB 34 does not permit California LEAs to share ALPR information with private entities or out-of-state or federal agencies, including out-of-state and federal law enforcement agencies."[1] Nevertheless, in FY24 shared data with various out-of-state and federal agencies, including U.S. Customs and Border Protection. Furthermore, the ALPR data is stored on third-party servers operated by a Georgia-based company, Flock Safety. Use of this third-party vendor poses additional risks for federal law enforcement agencies, including immigration authorities, to access this data.
    - The audit policy under the Use Policy and discussed in the Annual Report is too broad, cursory, and reactive. As discussed in the Overall Concerns section of this document, specific audit policies and KPIs are needed.
- (3) use of the surveillance technology, in accordance with the approved Surveillance Use Policy, should **cease until modified** to address identified concerns.

[1] https://oag.ca.gov/system/files/media/2023-dle-06.pdf.

- 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.
- **The Council should order all use of ALPR data cease until the above four amendments are made.**

Unmanned Aerial Systems (drones)

- (2) civil rights and civil liberties **are not** being safeguarded;
    - The Use Policies for the various UAS technologies must be refined to prohibit deployment at public demonstrations.
    - Last year, SDPD used UAS systems at three civil demonstrations. Such use is unacceptable absent a specific, unique threat to public safety is present.
- (3) use of the surveillance technology, in accordance with the approved Surveillance Use Policy, should **be modified** to address identified concerns regarding use of UAS technology at public demonstrations.

PTZ Cloud Based System, Trail Cameras, and Covert Audio/Visual Recording Devices:

- (1) **it is not known if** the benefits to the community of each item of approved surveillance technology outweigh the costs;
    - None of these technologies, per the SDPD Annual Report, were used during FY24.
    - The SDPD refused to disclose how many of these devices the Department maintains.[2]
    - Therefore, PAB cannot evaluate what the costs of these technologies are.
- (3) use of the surveillance technology, in accordance with the approved Surveillance Use Policy, should **continue** with the expectation that such figures are reported going forward.

The PAB cannot fully evaluate any technologies—including those discussed above—until provided with the requested KPIs, detailed audit policies, and process for establishing when "exigent circumstances" exist. The PAB looks forward to working with SDPD to ensure the Department addresses these requests in a manner that best benefits the community.

Cc: SDPD Chief Wahl
Kohta Zaiser

[2] https://www.sandiego.gov/sites/default/files/2025-03/sdfd-response-to-pab-questions-022025.pdf. This operational-security-citing refusal to provide data was repeated in-person by the SDPD in meeting with the PAB.