Surveillance Impact Report
Products Received from City Departments
San Diego City Attorney's Office

DESCRIPTION:

The San Diego City Attorney's Office (SDCAO) Civil Divisions may receive information from other City departments collected through the use of Surveillance Technology (Products of Surveillance Technology, or PST). The purposes for the SDCAO Civil Divisions receiving Products of Surveillance Technology include the investigations of incidents posing the risk of City liability, responding to civil litigation statutory discovery demands, investigations in support of consumer or tenant protection actions, and investigations supporting actions for Gun Violence and Workplace Violence restraining orders. One example of Products of Surveillance Technology received by the SDCAO Civil Divisions is the video/image files from the San Diego Police Department's Body Worn Cameras (BWC). For the same purposes, Unmanned Aircraft Systems (UAS) video/images/data, may also be received by the SDCAO Civil Divisions.

PURPOSE:

This technology is used by the San Diego City Attorney's Office (SDCAO) Civil Divisions to obtain information regarding parties, witnesses, claims, defenses, and damages in active and anticipated litigation, especially those in which City personnel were present at an incident that led to legal action, regardless of whether they were parties named in the action. These Products of Surveillance Technology allow the SDCAO to fully evaluate claims and fulfill its Charter obligations to the City.

LOCATION:

The SDCAO does not collect information from any location that is entered into Products of Surveillance Technology received from City Departments. PST is used by the Civil Divisions of the SDCAO in cases where the City of San Diego is involved in civil litigation, restraining orders, or code compliance. PST are accessed by SDCAO authorized employees via SDCAO computers, both in the SDCAO work site and remotely, with mandatory security protocols in place, such as the City's Virtual Private Network and Multi-Factor Authentication. The work sites of the SDCAO are in secure, access-controlled buildings.

IMPACT:

The SDCAO's Surveillance Use Policy for PST received from City Departments safeguards civil liberties and civil rights. PST uses are not based on discriminatory or viewpoint-based factors. The SDCAO's use of surveillance technology is intended to support and benefit the City of San Diego while minimizing and mitigating potential impacts on community members' civil rights and civil liberties. It is used only in performing legal services for the City.

Surveillance Impact Report
Products Received from City Departments
San Diego City Attorney's Office

MITIGATION:

The collection, use, retention, or dissemination of data shall not be used to violate the Constitutional rights of any person or be used in any manner that would discriminate against any person based upon their ethnicity, race, gender, national origin, religion, sexual orientation or gender identity. Data is only shared when required by law or due process. A protective order may be sought for this data when it is appropriate to protect the interests of the city and citizens of San Diego.

DATA TYPES AND SOURCES:

The types and sources of Products of Surveillance Technology received from City Departments would be the same as those approved by the City Council for that City Department.

DATA SECURITY:

SDCAO computers require user login authentication and are situated in secure buildings with access control. When working remotely, authorized users are required to login via the City's Virtual Private Network using a work computer and multi-factor authentication. Only authorized employees of the SDCAO shall access the data. When obtaining and transferring PST, the SDCAO will use an approved secure file sharing application with password protection or transfer data via secure USB drives/CD-ROMs with password protection.

FISCAL COST:

There is no fiscal cost associated directly with PST received from City Departments. The various City Departments pay for the technologies and the SDCAO may obtain the products as part of a Civil Division case investigation. When necessary, the SDCAO may purchase USB flash drives to provide for the secure and efficient exchange of the PST received from City Departments; the estimated cost for these USB Drives is less than $100 per year. The SDCAO has a secure file-sharing method as part of its Information Technology (IT) contracted services.

THIRD PARTY DEPENDENCE:

The types and sources of Products of Surveillance Technology received from City Departments would be the same as those approved by the City Council for that City Department. The SDCAO has a secure file-sharing method as part of its Information Technology (IT) contracted services.

Surveillance Impact Report
Products Received from City Departments
San Diego City Attorney's Office

ALTERNATIVES:

There are no alternatives to using Products of Surveillance Technology received from City Departments. If data obtained from these products is involved in a case assigned to the SDCAO, the SDCAO will need to obtain copies of that data to prepare an adequate case on behalf of the City and citizens of San Diego.

TRACK RECORD:

The SDCAO has a history of successfully collaborating with City Departments in identifying and obtaining information critical to City litigation.

There are no known instances of these technologies being used adversely by the SDCAO in any manner that would abuse the civil rights or civil liberties of persons. There are no known controversies or court rulings for or against the SDCAO's use of Products of Surveillance Technology received from City Departments.

PUBLIC ENGAGEMENT AND COMMENTS:

On September 23, 2026, at 12:00 p.m., there was a publicly held meeting broadcast live and facilitated in person in all nine Council Districts in the City of San Diego. The following surveillance technologies were presented by the SDCAO:

1. Aggregate Public Records Search Systems
2. Automated Regional Justice Information Systems
3. Products Received from Law Enforcement
4. SDLaw
5. FinCEN Query

The SDCAO video recorded this meeting so that it could be presented to a larger group. The benefit of the video was the capability of translating the presentation into over 100 languages such as Spanish, and other languages frequently used by the communities within San Diego, to maximize penetration of the materials to affected groups. The link to the video (TRUST Community Meeting - City Attorney's Office) is at:
https://www.youtube.com/watch?v=QOkigc7fNdw

There were eight attendees in San Diego City Council District 3. There were no attendees in any of the other districts.

There were six public comments and no questions out of the eight attendees. There were no comments submitted to the online public comment form.

Surveillance Impact Report
Products Received from City Departments
San Diego City Attorney's Office

Comment #1:

The speaker strongly opposed San Diego's continued use and funding of surveillance technologies such as ARJIS and ALPRs [Automated License Plate Recognition systems]. The speaker argued that these tools enable unrestricted data harvesting, violate civil rights, and were designed to circumvent protections rather than enhance safety. The speaker emphasized that surveillance and AI systems are inherently dangerous, cannot be responsibly regulated, and disproportionately harm vulnerable communities, especially in the context of ICE actions. The speaker concluded by urging elected officials to address these concerns and reaffirmed that the community will continue holding leaders accountable.

Comment #2:

The speaker expressed concern that technological progress should serve the public, not powerful interests. The speaker highlighted a report showing thousands of ALPR search entries labeled only as "other," which the speaker argued enables misuse despite supposed safeguards. The speaker stated that ambiguous search categories and limited auditing allow systems like ARJIS to be abused by malicious actors. The speaker stressed that subjective assurances of ethical data practices are insufficient and called for an end to the city's use of these surveillance technologies.

Comment #3:

The speaker spoke about how surveillance technology contributes to systems of displacement. He criticized the meeting's timing and short notice as a form of manufactured consent that limits public participation. The speaker also warned against relying on arrest data, noting that many arrests are biased or unconstitutional and should not inform surveillance systems. The speaker raised concerns about offsite access to these tools through VPNs and underscored that both the technologies and the processes surrounding them are deeply problematic.

Comment #4:

The speaker argued that San Diego must rethink its approach to surveillance technology. The speaker described a pattern in which society embraces new technologies without understanding their long-term consequences, using smartphones as an example. The speaker noted that individuals can control their personal devices, but government surveillance systems offer no comparable control to the public. The speaker urged leaders to follow a "do no harm" principle when implementing advanced technologies and stressed the need for transparency under the Trust Ordinance. The speaker stated that while harms from ALPRs are already known, the community still lacks critical information about ARJIS and its use.

Comment #5:

The speaker expressed frustration that the city has not followed the processes outlined in the Trust Ordinance, despite its unanimous approval. The speaker said the annual report, which passed the Privacy Advisory Board, still has not been presented to the City Council, calling this a failure of accountability. The speaker noted that required use policies and reviews for existing technologies have not occurred and criticized the city for discussing even more powerful surveillance tools without adhering to proper procedures. The speaker voiced deep concern about the impact on communities already facing risks from ICE actions and stated that the city is not taking the issue seriously.

Comment #6:

The speaker raised concerns that new surveillance technologies consistently bypass the Privacy Advisory Board, undermining its role in ensuring transparency and accountability. The speaker warned that powerful entities, including large corporations and investors, may gain access to sensitive data, which could be exploited in harmful ways. Drawing comparisons to surveillance systems in other countries, the speaker cautioned that data could be weaponized to restrict essential services or freedoms. The speaker argued that the government's partnerships with wealthy corporations contradict claims of avoiding such alliances and urged the city to scrutinize where data is being sent and how it might be used.

At an evening meeting on September 24, 2026, at 5:30 p.m., the SDCAO re-broadcast the recorded video from September 23, 2026. The link to the video (TRUST Evening Community Meeting City Attorney's Office) is at: https://www.youtube.com/watch?v=M2uG7aHxfw0

For the evening meeting, there were two attendees in San Diego City Council District 3 and four attendees virtually.

There were two public comments and no questions from the attendees. There were no comments or questions submitted to the online public comment form.

Comment #1:

The speaker expressed deep appreciation for meeting host and the City Attorney's Office for their presentation on surveillance technology. They described feeling overwhelmed by the information but grateful for gaining a new awareness of privacy and surveillance. They now recognize that monitoring is constant once they leave their home and commit to being more alert while staying open to emerging technology. They closed by reaffirming their long-time support for the PAB [Privacy Advisory Board], expressing love for its work, and sharing excitement about attending an upcoming meeting.

Comment #2:

The speaker thanked the group for hosting the public forum and praised the presenter for balancing civil data collection topics with law enforcement considerations, such as "SARS" reporting and coordination with county sheriffs. The speaker raised concerns about data retention, referencing a state bill that would require judicial warrants for accessing personal data. The speaker questioned whether the standard of expunging data after 30 days is genuinely practiced and encouraged deeper discussion on both warrant requirements and long-term data retention in future PAB [Privacy Advisory Board] meetings.