Surveillance Impact Report
SDLaw
San Diego City Attorney's Office

DESCRIPTION:

SDLaw is the San Diego County Sheriff's Office extranet platform that hosts a comprehensive suite of law enforcement and criminal justice applications shared with local, state, and federal law enforcement and justice partners. Access to SDLaw applications is restricted to authorized users who have completed California Law Enforcement Telecommunications System (CLETS) certification. SDLaw is a secure web site with several web-based applications such as APPS (Arms Prohibited Person System), eJIMS (Jail Information Management System), eLab Results, eRO (Restraining Orders), eWarrant, eSUN, and SDFusion.

PURPOSE:

SDLaw is used by the Civil Divisions of the San Diego City Attorney's Office (SDCAO) to perform fact investigation for assigned cases in which the SDCAO is defending the City in civil litigation, to investigate fraud, consumer protection complaints, violations of the California Unfair Competition Law (UCL), building code violations, or substandard living conditions; to pursue a restraining order, or to secure firearm relinquishment. Access to the system is granted by the SDCAO CLETS Coordinator/account manager. Use of the system is based on a "right to know, need to know" basis, meaning that the employee accessing the system is both authorized to use it based on their specific work duties and are using it only for investigation of a specific case or task assigned to them. The use of SDLaw is an essential component of case investigation that both enhances and advances the investigative process; it is used extensively by sworn and non-sworn law enforcement, corrections, community corrections, and regulatory employees throughout San Diego County.

LOCATION:

The SDCAO does not collect information from any location that is entered into SDLaw. SDLaw 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. SDLaw is 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. SDLaw is a web-based set of applications that must be accessed via a secure network connection.

IMPACT:

The SDCAO's Surveillance Use Policy for SDLaw safeguards civil liberties and civil rights. SDLaw 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.

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. SDLaw provides efficient and time-saving access to law enforcement records, many of which are public records and/or open-source information, but with additional details. SDLaw does not utilize visual or audio recording capabilities or use facial recognition.

DATA TYPES AND SOURCES:

The SDCAO does not enter data into SDLaw. The SDCAO reviews information from other sources as outlined below. SDLaw contains local jail booking data, local warrant and restraining order data. It also provides links to state and federal data Criminal Justice Information Systems databases.

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.

FISCAL COST:

The SDCAO does not pay separate fees to the San Diego Sheriff's Office for access to SDLaw and eSUN applications. The San Diego Police Department's (SDPD) fee covers access for all users in the City of San Diego.

THIRD PARTY DEPENDENCE:

The SDCAO does not store data in SDLaw. SDLaw is managed by the San Diego Sheriff's Office (SDSO) and a data-sharing agreement has been in place between SDSO and the SDCAO since 2005. The SDSO is also the County Control Agency overseeing agency access to the California Law Enforcement Telecommunications System (CLETS), which in turn can access

the National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications System (NLETS). SDLaw retains a user's search terms and case reference for audit purposes. All data stored within the platform is restricted and only accessible to authorized persons. Information can be accessed by the SDCAO user and saved in secure network drives managed by the SDCAO. No data will be stored on City hardware or network drives unless downloaded from the web application for use in a qualifying investigation.

ALTERNATIVES:

There are no alternatives to using SDLaw. It is the designated application that provides local jail booking, warrant, and restraining order information, as well as other local information outlined in the Data Types and Sources section above. The SDSO is the state-designated agency that provides the regional gateway to CLETS, NCIC, and NLETS data for law enforcement agencies in the region.

TRACK RECORD:

The SDCAO has used SDLaw applications successfully for more than 20 years. The SDCAO uses SDLaw multiple times each day to conduct authorized case investigations. There is no known adverse information regarding the use of SDLaw, nor are there known lawsuits involving this application.

SDCAO staff use SDLaw to check local restraining orders in order to evaluate Gun Violence Restraining Order referrals and failure to comply with relinquishment of firearms after issuance of a Non-Compliance Order from the court. SDCAO also use SDLaw to access the state's Automated Firearms System to determine if persons have relinquished firearms pursuant to GVROs or Domestic Violence Restraining Orders (DVROs) or other restraining orders.

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

Surveillance Impact Report
SDLaw
San Diego City Attorney's Office

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.

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.

Surveillance Impact Report
SDLaw
San Diego City Attorney's Office

Comment #1:

The speaker expressed deep appreciation for meeting host and the City Attorney's Office for their presentation on surveillance technology. They describe 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.