Revised Annual Report

Automated License Plate Recognition (ALPR)
San Diego Police Department

Department/Division: Police - Special Project and Legislative Affairs

Related Policy/Procedure:

- DP 1.51 Automatic License Plate Recognition (ALPR)
- DP 3.02 Property and Evidence

Revised August 1, 2025

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

ALPR systems have proven to be powerful and effective tools for the San Diego Police Department, helping officers identify suspect vehicles, solve cases faster and use resources more efficiently.

Last year, ALPR technology played a critical role in the arrest of 208 suspects and the recovery of an estimated $3 million in stolen property, including 223 stolen vehicles and 10 firearms. The system helped locate a missing man with dementia, apprehend a suspect wanted for attempting to kidnap two children, and track down suspects in a series of hate crimes in Hillcrest.

Officers have used ALPR images and data in over 140,000 investigative queries, supporting efforts across divisions, council districts, and with partner agencies throughout the City and County of San Diego. The technology played a key role in 294 cases and has strengthened collaboration and expanded investigative reach.

This technology supports precision policing. It reduces the need for broad patrols, helping officers focus their efforts and avoid unnecessary stops, saving both time and resources. ALPR has also become a valued, industry-standard tool that supports officer recruitment and retention.

The San Diego Police Department remains committed to using ALPR technology responsibly and transparently to enhance public safety while protecting civil liberties.

Notes: Need a clear, plain-language description of the technology, what it does (reads license plates, takes images, processes gathered data, analyzes it to determine make/model/color of vehicle, matched with license plate information, etc., how it functions (hardware, software, vendor, system architecture), and quantity of information gathered. Explain reasons for the seemingly large amount of data collected (reads every plate/vehicle). Place numbers put it in context.

Provide specific examples of use in practice (e.g., types of investigations supported, outcomes). Put into context and explain the 140,000 queries v. the

Commented [MS1]: Ensure referential integrity with the Ordinance and the Use Policy.

Commented [MS2]: How is this measured or determined?

Commented [MS3]: How is this assessed?

Commented [MS4]: Have metrics been established regarding the number of queries vis-a-vis the number of arrests or recovery of stolen property?

Commented [MS5]: How is this term being defined? I like the term.

Commented [MS6]: How is this measured?

number of arrests and amount of vehicles/firearms recovered. In other words, the number of queries seems high for the number of arrests/property, so explain why. Explain benefits beyond arrests maybe? Include total number of plates/vehicles captured, along with the other data (e.g., "In FY24, 1.2 million plates captured; 1,400 alerts generated; 72 confirmed as investigative leads").

Explain its limitations and potential privacy/civil rights/civil liberty risks, and how the Use Policy ensures functioning within those limitations and in a way that avoids the risks.

In this section or elsewhere in the report, add quantitative detail: how many plates were captured, how many alerts generated, how many hits confirmed; assessment of how unnecessary data was minimized.

Whether here or elsewhere, explain evidence of compliance with use policy (audit results confirming timely purging), number/percentage of records retained past 30 days as evidence, vendor role in deletion process.

SHARING OF DATA: Whether and how often data acquired through the use of the surveillance technology was shared with any non-City entities, the name of any recipient entity, the types of data disclosed, under what legal standards the information was disclosed, 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.

In addition to providing ALPR data to the District Attorney's Office for criminal prosecution, SDPD accessed or shared ALPR images or data with other law enforcement agencies after a qualifying crime had occurred, such as a homicide or shooting, and when there was a legitimate investigative need.

In a few serious cases last year involving crimes such as human trafficking, an assault against an officer and crimes against children, the Department shared ALPR data with out-of-state and federal law enforcement agencies. None of the qualifying crime cases were related to immigration enforcement. (See Addendum A for a comprehensive list of outside agency data sharing.)

After receiving guidance from the California Department of Justice, SDPD immediately ended all such sharing with federal and out-of-state departments. This decision was formalized in a Department-wide order in May 2025.

Additionally, SDPD identified a brief period after system launch during which other California law enforcement agencies could temporarily access SDPD's ALPR data. As the

Department discussed in a memo issued to the Privacy Advisory Board and each member of City Council on June 13, 2025, this period was mistakenly left out of the Annual Surveillance Report and has been added to the Unauthorized Access section below.

These changes reflect the Department's commitment to responsible technology use and public trust.

Notes: Include legal authority citation that allows sharing and the authority that prohibits/limits sharing. Add number of requests that were denied and reason.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES: 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.

There have been no updates, upgrades, or configuration changes that expanded or reduced the surveillance technology's capabilities.

ANNUAL 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.

These costs are duplicates of the Smart Streetlight (SSL) costs as this is an embedded technology, and the cost is built into the SSL costs.

On 12-26-2023 an initial payment of $3,512,500 was paid for installation and one (1) year on service for the 500 Smart Streetlights with embedded Automated License Plate Recognition technology.

On 6-24-2024 a payment of $6,800 was disbursed for relocation of SSL/ALPR units.

On 12-11-2024 a payment of $1,449,602.08 was authorized for calendar year 2025 contract obligations.

All funding sources were from the City's General Fund.

Notes: Provide a more detailed description of the relationship between Smart Streetlights and ALRP's, such as, there is one contract and the ALPR's are provided through a different vendor, but contractually through an addendum to the Smart Streetlight contract. Again, the idea is to provide a response that explains the relationship to someone otherwise unfamiliar with it.

INSTALLATION LOCATION: A description of the physical objects to which the surveillance technology hardware was installed, if applicable, and

Commented [MS7]: What about security or routine patch management changes? How are those logged, assessed for risk, and validated?

Commented [YD8]: What security measures does Flock Safety use WRT supply chain security for their software and hardware?

Commented [YD9]: What is the breakdown for the costs WRT installation, maintenance, data storage, software licenses, access and network feeds, indirect costs for transparency?

without revealing the specific location of the hardware, and a breakdown of the data sources applied or related to the surveillance technology software.

The Smart Streetlights with embedded ALPR technology were attached to City of San Diego streetlight poles.

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

The Smart Streetlights with embedded ALPR technology were deployed Citywide in all police divisions.

Current camera deployment locations can be found at the link below.

- https://webmaps.sandiego.gov/portal/apps/webappviewer/index.html

Notes: Make sure website is up to date.

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.

Since SDPD's ALPR program launched, some community members have raised concerns including over how the technology protects people's privacy, if it could be used in immigration or reproductive rights investigations, and whether the data collected would be vulnerable to outside access.

SDPD has taken these concerns seriously. We've worked to educate the public, strengthen policies, and partner closely with the Privacy Advisory Board to ensure the community can feel confident this technology is being used responsibly to keep our neighborhoods safe.

Additionally, the Department received a letter dated July 31, 2024, from the Community Advocates for Just and Moral Governance titled "Notice of Violations of the TRUST Ordinance – Smart Streetlights and Automated License Plate Readers." No other written complaints or concerns have been filed with the Department.

The Department remains committed to working with community groups, the Privacy Advisory Board, and elected officials to ensure continued public education and transparency around this technology. The Use Policy continues to outline clear safeguards to protect civil rights and civil liberties.

Notes: Provide more detail/description of the history of complaints and a summary, especially give the history, so that someone generally unfamiliar with the history would be brought up to speed.

AUDITS OR INVESTIGATIONS: The results of any internal audits or internal investigations relating to surveillance technology, information about any violation of the Surveillance Use Policy, and any action taken in response. To the extent that the public release of this information is prohibited by law, City staff shall provide a confidential report to the City Council regarding this information to the extent allowed by law.

Several months after the system's launch, a supervisor of the Special Projects and Legislative Unit began conducting weekly audits of the entries filed when individuals would access the technology. These audits revealed inconsistencies in the metadata of these entries, resulting in several audit improvements, including one that was piloted in San Diego and has now become standard practice across Flock's network. (Flock is the subcontractor that provides the ALPR equipment and services.)

In the Flock Safety interface, users conducting a search of ALPR data were required to enter a

Commented [LD10]: I recommend you list the core risks that you are "auditing" for such as compliance with the user policies related to access to system and data, backup, retention, and compliance with local and state laws including SB 54, etc
Note briefly the "audit process" by noting that the reviews are done by someone independent of the officers performing the tasks, issues are tracked and elevated and followed-up (NOT one-off findings).
Would it be beneficial to have the City auditor help as a one-off to write some audit steps and processes to demonstrative independence of thought?

Commented [YD11]: Are there APIs for third party use, if yes, how are those secured?

"Reason" for the search, but it did not prompt users to include a case or incident number. Because of this, users provided appropriate reasons for a search, which is in line with the Department's Surveillance Use Policy, but because there was not a more detailed prompt, more specific information was omitted.

To address this, on January 26, 2024, the audit issued ORDER OR 24-04, which requires all ALPR users to:

- Include a specific case number or incident number in the "reason" field when conducting searches.
- Ensure the event is linked to a specific crime (broad entries like "11-86" are no longer acceptable).
- Add relevant details to assist with investigative documentation and future court proceedings.

Because this update was implemented after system launch, it took users time to adjust. However, any time a user conducted a search without the appropriate metadata, a supervisor immediately addressed the issue. All searches were verified to be connected to an active case number or event number in compliance with the Use Policy.

SDPD also worked with Flock Safety to create a new, dedicated "Case/Incident Number" field in addition to the "reason" field. This section was added to the Flock Safety interface nationwide, resulting in more thorough entries and audits.

The Department Order is part of this year's Annual Training related to the ALPR system and will be rolled into annual training moving forward.

As previously discussed, another kind of internal audit identified the period at our system's launch when an improper setting mistakenly allowed California law enforcement agencies to access SDPD's ALPR data in late December 2023 to early January 2024. That setting was immediately corrected and hasn't occurred since.

This incident motivated the Department to build on its audit process by including the Department's Research, Analysis and Planning Unit (RAP) (the Department's internal auditing and controls unit) earlier in the process and by mandating quarterly audits. On April 25, 2025, a Department Order was issued requiring surveillance technology Subject Matter Experts (SME) to conduct these enhanced audits.

As part of this process:

- All SMEs will conduct quarterly audits of the requirements in the Annual Report to enhance record keeping and ensure greater accuracy of the Annual Report.
- Department SMEs will conduct audits at random for uses of the technology.
- The Department will create share logs to document what data is shared and why.
- RAP will conduct independent audits to confirm share logs are completed, ensure that use policies are current, and ensure that system user access is up to date.
- Any violation will be immediately reported to RAP for documentation and corrections.

DATA BREACH DETECTION: A general description of all methodologies used to detect incidents of data breaches or unauthorized access, 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.

SDPD works closely with the City's Department of Information Technology (IT) to assess cybersecurity risks, approve technology, and ensure proper governance. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

Key safeguards in place:

Commented [MS12]: How many such cases occurred?

Commented [MS13]: Excellent.

Commented [MS14]: How has this been verified? Please see the previous comment regarding authentication, session expiry settings, etc.

Commented [LD15]: There are several "incidents" noted in these paragraphs. However, it would be good to have a brief summary of ALL reviews or audits such as "Reviewed XX number of queries", " reviewed for proper qualifications of all users accessing the system," etc.

Commented [LD16]: Again. Recommend a short statement to identify what the "audit" is covering. People will question the rigor of the audit. Thus, you should note and keep data on samples looked at, results of each of the audits and resulting corrective actions.

Commented [MS17]: With whom?

Commented [LD18]: This section needs to include audit of the controls around the underlying data with Flock. Or Ubicquia Need to ensure you annually receive a service center audit under SSAE 18 for a SOC 2, Type 2 audit.

All ALPR data is stored in secure law enforcement facilities with multiple layers of physical and digital protection.

Encryption, firewalls, and authentication protocols are used to protect all digital evidence.

Access is strictly limited to SDPD personnel in investigative or enforcement roles, and only those authorized by the Chief of Police may access ALPR data.

Flock Safety also follows strict data security protocols and undergoes regular third-party audits. Their system uses Amazon Web Services (AWS), a cloud platform built for high-level government security. Flock uses advanced encryption (256 bit), role-based access, and is CJIS-compliant. They maintain multiple third-party certifications, including SOC 2 (Type II), SOC 3, and ISO 27001. All ALPR data downloaded from a video management solution to a mobile workstation or to digital evidence storage like Axon evidence is only accessible through a login/password-protected system capable of documenting all access of information by name, date and time.

Notes: The first paragraph probably is not technically accurate. Flock is the entity responsible for data storage, breach prevention, and breach notification of the database. The use policy should be updated to reflect that Flock will provide periodic updates on whether there has been any breach or other unauthorized access at the point of data storage. Also, note that the data base is known as the AWS GovCloud.

Add statistics on access (number of queries performed, by whom, for what purposes), Any violations or improper access incidents, detail on log auditing results. Report aggregate access logs (e.g., "4,215 queries made by 37 officers; all consistent with policy; no unauthorized access incidents found").

Commented [YD19]: Can they include more details with visual diagrams of this (with security considered where applicable)?

Commented [MS20]: Is Flock deployed to AWS' government cloud?

Commented [YD21]: Excellent inclusion here. How are the status of these certifications verified for compliance?

Commented [MS22]: Is the authentication only user name and password or does it require MFA? Separately, what are the password complexity requirements and are they enforced technically?

How frequently are passwords rotated? Is the Flock system part of a single sign-on (SSO) service used by the SDPD or the City?

DATA BREACH OR UNAUTHORIZED ACCESS: 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.

Although California law permits ALPR database access between California agencies, the City's Contract and Use Policy for ALPR bars outside agencies from accessing SDPD's ALPR Flock database. While there was no data breach, there was a brief period of unauthorized access by other California law enforcement agencies due to a system configuration error at the system's launch.

As a result of the system misconfiguration, from December 29, 2023, to January 17, 2024, SDPD's ALPR camera system was inadvertently included in 12,914 searches conducted by other state agencies. No out-of-state or federal law enforcement agencies had access to data during this period. While an additional 795 searches were conducted on December 28, 2023, none of the Department's cameras had been turned on, so there was no data available to search.

Of the 12,914 searches conducted by other state agencies, 12,202 were for a specific license plate or partial license plate, and around 50 percent were repeated inquiries for the same license plate wanted in connection with an investigation.

Below is a table showing the number of cameras active on each day and the number of searches conducted by other state agencies:

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

Search Timeframe	Number of Searches
2023 Searches	3,073
2024 Searches	10,536
Total	**13,609**
December 28, 2023, Searches	-795
Actual Searches	**12,914**

The initial unauthorized access was discovered through an internal audit on or around January 17, 2024. The Department immediately notified Flock, which corrected the data-sharing settings the same day. This issue has not occurred since.

Notes: Add that Flock has informed the SDPD that there have been no data breaches. State whether there is any independent verification or results of security testing (Flock should be able to provide this). Get from Flock details on encryption type, vendor certifications (e.g., CJIS, FedRAMP)

Commented [YD23]: And include if the data breaches affects other agencies to avoid watering hold attacks.

Commented [LD24]: This can be accomplished via the SOC 2, Type 2 audit of the data centers noted above.

INFORMATION AND STATISTICS: Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. Accessible via this webpage is the City's neighborhood crime summary dashboard: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also

available on this site are dictionaries to help navigate the different data sets.

Investigation Assists	
187	7
211	6
207	3

245DV	1
245	5
261	2
288	3
459	10
Traffic	3
Other	10

ALPR Responses	
10851 Recovered	223
10851 In Custody	175
SDPD Hotlist	18
Missing Persons	1

Totals	
Total Events	294
Total In Custody	208
Estimated Recovered Value	$3,055,400
Recovered Guns	10

Notes: Consider deleting references to general crime statistics as it does not directly answer the ordinance question. Alternatively, add it to the end and make clear that it is added to provide further related information. Consider adding a narrative description that explains whether the surveillance technology has been effective at achieving its identified purposes in addition to statistics. That is, why does the SDPD like these and find them useful?

CALIFORNIA PUBLIC RECORDS ACT REQUESTS: 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.

There were five Public Records Act requests related to ALPR in calendar year 2024:

Commented [MS25]: What is the difference between the 'Request Date' and the 'Closed Date?'

Is there non-repudiation for access and clear attribution to the entity and authorized user?

Request Number	Request Date	Closed Date
24-1400	2/23/2024	4/16/2024
24-6236	9/10/2024	9/14/2024
24-6912	10/6/2024	10/20/2024
24-7450	10/24/2024	10/24/2024
24-7913	11/12/2024	11/16/2024

Notes: How many have been denied in whole or in part, and if so, the reasons? Are full responses given to all the PRA's? If yes, so state. If not, describe generally why some requested information is not provided.

REQUESTED MODIFICATIONS TO THE USE POLICY: Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

The following modifications to the Automated License Plate Recognition Use Policy are proposed.

- Add reference to California Senate Bill 34 under the subsection that defines prohibited ALPR uses including those that violate federal, state or local laws.
- Add to the Third-Party Data Sharing section that ALPR data shall not be shared with private entities or out-of-state or federal agencies, including out-of-state and federal law enforcement agencies in accordance with SB 34.
- Replace references to "Special Projects and Legislative Affairs" & "SPLA" with "program administrator."
    - This change aligns with the new SDPD command structure.
- Remove section with header "Modifications to the Use Policy."
    - This change aligns this use policy with all other SDPD technology use policies. Modifications to a Surveillance Use Policy are governed by the Transparent and Responsible Use of Surveillance Technology Ordinance.
- Other additional typos and language corrections. These corrections do not have an impact on the use of the technology.

Notes - consider adding periodic reports from Flock regarding security issues, including data breaches and other unauthorized access

ADDENDUM A – OUTSIDE AGENCY SHARING

HOW SDPD HANDLES ALPR SEARCH REQUESTS

SDPD does not grant outside agencies direct access to its ALPR system. When another law enforcement agency needs assistance, they must contact SDPD, explain the qualifying reason for the request (such as a serious crime or public safety emergency), and then SDPD personnel conduct the search internally. The requesting agency is then informed of the relevant result, including whether no information was found.

The only exception to this process occurred during the three-week period following system launch when a configuration error temporarily allowed other California law enforcement agencies to search SDPD's system directly. That issue was identified and fixed in January 2024.

Commented [YD26]: Are they Data Sharing Agreements for this and if yes, what are the stipulations?
Are there audit reviews and measures in place for compliance?
Can there be metrics on denied requests if the qualifying reasons are not apt for such request?

SEARCHES CONDUCTED DURING THREE-WEEK LAUNCH PERIOD

California Agency	Times Shared
Alameda County Sheriff's Office	307
Alhambra Police Department	31
Anaheim Police Department	11
Anderson Police Department	4
Atherton Police Department	1
Auburn Police Department	4
Azuza Police Department	1
Bakersfield Police Department	5
Baldwin Park Police Department	33
Beaumont Police Department	71
Bell Gardens Police Department	1
Benicia Police Department	7
Beverly Hills Police Department	5
Brea Police Department	14
Brisbane Police Department	3
Buena Park Police Department	59
Burbank Airport Police Department	4
Burbank Police Department	21
Chino Police Department	56
Cal Fire	10
Cal State Fullerton	1
California Highway Patrol	91
Campbell Police Department	1
Capitola Police Department	33
Cathedral City Police Department	4
Citrus Heights Police Department	8
City of Riverside Police Department	11

Claremont Police Department	2
Colma City Police Department	6
Concord Police Department	2
Contra Costa County Sheriff's Office	168
Corona Police Department	102
Costa Mesa Police Department	10
Covina Police Department	65
Culver City Police Department	26
Cyprus Police Department	26
Danville Police Department	22
Delano Police Department	4
Dixon Police Department	12
East Bay Parks	12
El Cajon Police Department	2
El Centro Police Department	33
El Monte Police Department	220
Elk Grove Police Department	18
Escalon Police Department	8
Escondido Police Department	12
Fairfield Police Department	28
Farmersville Police Department	2
Folsom Police Department	10
Fontana Police Department	153
Fort Bragg Police Department	2
Freemont Police Department	24
Galt Police Department	5
Garden Grove Police Department	144
Gilroy Police Department	40
Glendale Police Department	8
Glendora Police Department	61
Grass Valley Police Department	11
Hanford Police Department	7
Hayward Police Department	60
Hemet Police Department	4
Hercules Police Department	69
Hillsborough Police Department	2
Hollister Police Department	1
Huntington Beach Police Department	25
Imperial City Police Department	1
Imperial County Sheriff's Office	1
Indio Police Department	18
Irvine Police Department	104
Kern County Sheriff's Office	257

Kings County Sheriff's Office	17
La Habra Police Department	5
Laverne Police Department	5
Laguna Beach Police Department	36
Los Angeles County Sheriff's Office	564
Lincoln Police Department	2
Lindsay Public Safety Department	5
Livermore Police Department	35
Lodi Police Department	14
Los Angeles Police Department	104
Madera County Sheriff's Office	1
Marin County Sheriff's Office	9
Mendocino County Sheriff's Office	2
Menifee Police Department	1
Menlo Park Police Department	32
Merced County Sheriff's Department	8
Monrovia Police Department	18
Montclair Police Department	36
Monterey County Sheriff's Office	7
Monterey Park Police Department	1
Moraga Police Department	7
Morgan Hill Police Department	150
Mountain View Police Department	31
Murrieta Police Department	220
Napa County Sheriff's Office	77
Northern California Regional Intelligence Center	53
Newark Police Department	21
Newport Beach Police Department	9
Novato Police Department	1
Oakley Police Department	16
Orange County Sheriff's Office	1225
Oceanside Police Department	8
Ontario Police Department	69
Orange Police Department	37
Orange County District Attorney's Office	8
Oxnard Police Department	21
Palm Springs Police Department	20
Palo Alto Police Department	23
Pasadena Police Department	1
Placentia Police Department	22
Placer County Sheriff's Office	56
Pleasanton Police Department	1
Pomona Police Department	51

Porterville Police Department	11
Redlands Police Department	8
Redwood City Police Department	83
Rialto Police Department	15
Rio Vista Police Department	53
Riverside County District Attorney's Office	19
Riverside County Sheriff's Office	2037
Rocklin Police Department	12
Sacramento District Attorney's Office	10
Sacramento Police Department	20
Salinas Police Department	3
San Bernadino County Sheriff's Office	208
San Bruno Police Department	122
San Diego Sheriff's Office	117
San Francisco Police Department	121
San Juaquin County Sheriff's Office	145
San Leandro Police Department	3
San Louis Obispo Police Department	7
San Mateo Police Department	60
San Mateo County Sheriff's Office	284
San Ramon Police Department	17
Santa Barbera County Sheriff's Office	270
Santa Clara Police Department	202
Santa Cruz Police Department	2
Santa Maria Police Department	36
Santa Monica Police Department	1
Santa Rosa Police Department	60
Seal Beach Police Department	1
Simi Valley Police Department	10
Solano County Sheriff's Office	255
Sonoma County Sheriff's Office	91
Stockton Police Department	33
Suisun City Police Department	2
Torrance Police Department	1
Tracy Police Department	84
UC Riverside Police Department	1
Ukiah Police Department	15
Union City Police Department	4
Upland Police Department	80
Vacaville Police Department	31
Vallejo Police Department	21
Ventura Police Department	62
Ventura County Sheriff's Office	41

Vernon Police Department	5
Visalia Police Department	57
Watsonville Police Department	25
West Covina Police Department	99
Wes Sacramento Police Department	3
Westminster Police Department	20
Whittier Police Department	6
Willits Police Department	2
Woodlake Police Department	26
Yreka Police Department	4

SEARCHES CONDUCTED BY SDPD FOR A CALIFORNIA AGENCY

California Agency	Times Shared
Alameda County Sheriff's Office	1
Anaheim Police	1
Belmont Police	1
Cal Automated Fingerprint Identification System	3
California Highway Patrol	19
Carlsbad Police	8
Chula Vista Police	51
Crime Stoppers	1
El Cajon Police	21
Escondido Police	6
Eureka Police	1
Huntington Beach Police	2
Imperial City Police	1
Indio Police	1
La Mesa Police	16
Long Beach Police	1
Los Angeles Airport Police	1
Los Angeles District Attorney's Office	1
Murietta Police	2
National City Police	61
Oceanside Police	7
Orange County Sheriff's Department	1
Redland Police	1
San Diego County Regional Auto Theft Task Force	4
San Diego Harbor Police	11
San Diego Sheriff's Office	99
San Diego Community College District Police	1

San Diego State University Police	2
University of California, San Diego Police	7
Whittier Police	3

SEARCHES CONDUCTED BY SDPD UPON REQUEST OF OUT-OF-STATE AGENCIES

Out-of-State Agency	Times Shared
Portsmouth Police (New Hampshire)	2

SEARCHES CONDUCTED BY SDPD UPON REQUEST OF FEDERAL OR INTERNATIONAL AGENCIES

Commented [MS27]: Just to confirm, these searches are now precluded by SB 34?

Federal/International Agency	Times Shared
Drug Enforcement Agency	20
Federal Bureau of Investigation	3
High Intensity Drug Trafficking Areas	1
Homeland Security Investigations*	4
Internet Crimes Against Children	3
Narcotics Task Force	60
U.S. Customs and Border Protection*	6
U.S. Marshals Office	3
U.S Probation	4
U.S. Secret Service	14
United States Postal Inspection Service	8
Violent Crimes Task Force	1
Royal Canadian Mounted Police	1
San Diego Human Trafficking Task Force	3
Violent Crimes Task Force	1

*These searches were not for immigration-related cases.