Surveillance Use Policy

Automated License Plate Recognition (ALPR)
San Diego Police Department

PURPOSE

Automatic License Plate Recognition Technology (ALPR) is a component of the San Diego Police Department's crime-fighting strategy that involves the identification of vehicles associated with suspects, witnesses, or victims. ALPR enhances the Department's ability to focus its investigative resources, deter the occurrence of crime, and enhance public safety of the community.

USE

Any integrations with additional technologies, such as facial recognition, or gunshot detection shall come to City Council for public review and approval, in accordance with the Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance, section 210.0103. Any modifications to this Policy must come to the City Council for public review and approval, in accordance with the TRUST Ordinance, section 210.0103. If Department Policy or Procedure conflicts with this Surveillance Use Policy, the Surveillance Use Policy will control.

ALPR systems have proven to be very effective tools in combating crime. The operation and access to ALPR data shall be for official law enforcement purposes only. The legitimate law enforcement purposes of ALPR systems include:

- Locating stolen, wanted, or subject of investigation vehicles.
- Locating vehicles belonging to witnesses and victims of a violent crime.
- Locating vehicles associated with missing or abducted children and at-risk individuals.
- ~~Department Procedure 1.51 for additional information regarding use guidelines for ALPR.~~

Department members shall comply with Department Procedure (DP) 1.51 and may be subject to discipline for violations thereof in accordance with City and Department rules and regulations.

When alerted via ALPR that a vehicle is wanted, stolen, or of interest to law enforcement, the user must:

(1) Visually ensure the plate was read properly and that the state of origin is consistent with the alert.

(2) Confirm the alert status of the license plate information via the NCIC database. This can be accessed through a secure device (e.g. vehicle laptop, cellular phone, desktop computer, etc.) or requesting the check through dispatch.

The following uses are expressly prohibited:

a. Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
b. Discrimination: It is a violation of this Policy to seek, submit, or retain ALPR information about individuals, or an organization, based solely on their religious beliefs, political affiliation, race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other classification protected by law.
c. Personal Use: It is a violation of this Policy to use the ALPR system for any personal purpose.

DATA COLLECTION

The San Diego Police Department will utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. All data and images gathered by the ALPR are for the official use of the department.

Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

The National Crime Information Center (NCIC) is the primary database for the entry and management of wanted vehicles/persons that ALPR technology utilizes, along with Department hot plate/hot lists related to criminal investigations.

Proactive manual entry of ALPR hot plates/hot lists is permitted with license plate information (i.e., BOLO or AMBER alerts) when it meets an authorized purpose. It is the responsibility of the department member who creates the hot plate notification to manage, edit, and delete the plate as necessary.

DATA ACCESS

Personnel authorized to use ALPR equipment or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. ~~Such personnel shall be limited to designated captains, lieutenants, sergeants, officers, detectives, and police department personnel unless otherwise authorized.~~ Authorized users include personnel listed in Department Procedure 1.51. Access will also be granted to supervisory staff of authorized users, (i.e., sergeants, lieutenants, captains) to ensure authorized users are complying with authorized usage, as well as Crime Analysts (backgrounded civilian non-sworn Department members) who enhance our investigations.

Authorized users under investigation for misconduct or criminal actions shall have their ALPR access revoked for the duration of the investigation and shall not have access restored until they have been cleared of wrongdoing.

DATA PROTECTION

Data collected by ALPR Technology shall be stored in a secured law enforcement facility with multiple layers of physical security and security protection. Encryption, firewalls, authentication, and other reasonable security measures shall be utilized to protect ALPR Technology data.

All ALPR data downloaded to the mobile workstation or in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time. Only those employees of the San Diego Police Department working in an investigative or enforcement function shall access ALPR data.

SDPD works with the City' s Department of Information Technology, which oversees the IT governance process. For additional details related to IT governance processes, which involves risk assessment, along with data and cyber security, refer to the information at the following link:

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

DATA RETENTION

All ALPR Technology data stored in the system shall be purged no later than 30 days from the date it was collected. Short retention period ensures that all data not associated with a crime is automatically deleted and unrecoverable. The vendor shall confirm monthly in writing the deletion of City of San Diego data from their systems.

PUBLIC ACCESS

ALPR data shall be made public or deemed exempt from public disclosure pursuant to state or federal law, refer to DP 1.51 for additional details related to the release of ALPR data.

THIRD PARTY DATA SHARING

~~ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, refer to DP 1.51 for additional details.~~

- ALPR data shall never be shared with Immigration and Customs Enforcement or Border Patrol for the purpose of enforcing immigration laws.
- ALPR data shall never be released to aid in the prosecution of an individual for providing, obtaining, or assisting in the provision or obtention of an abortion or any reproductive care.
- ALPR data shall never be shared with any federal taskforces which involve in any manner the investigation or prosecution of federal crimes, for conduct which is permitted under California law.
- No ALPR data shall be released to outside sources, except the San Diego City Attorney and San Diego District Attorney in accordance with legal proceedings or California law enforcement agencies for the purpose of investigating cross jurisdictional Part I crimes, until the adoption of a third-party data sharing use policy by the City Council.
- Nothing in this Policy should be interpreted as limiting the use of collected data for legitimate purposes by prosecutors or others legally permitted to receive evidence under law.

TRAINING

Training for the operation of ALPR technology utilized by the San Diego Police Department shall be provided by Police personnel or subject matter experts approved by the Department. All employees who utilize ALPR technology shall be provided a copy of this Surveillance Use Policy, along with instruction of the constitutional protections and case law requirements associated with its lawful use.

AUDITING AND OVERSIGHT

Personnel who are authorized to have access to the system shall be designated in writing and the designation shall ensure that their access to and use of the data complies with the Ordinance. A log shall be maintained that records when access to ALPR data is requested. This shall include the date, time, data record accessed, and staff member involved. The log shall be available for presentation for all required internal and external audits, and oversight will be maintained by the system Program Manager or their designee.

1. All evidence collected from the ALPR system is considered an investigative record for the Department and is for official use only.
2. Requests for ALPR data from the public or the media shall be processed in the same manner as requests for Department public records.
3. ALPR data that are the subject of a court order or subpoena shall be processed in accordance with the established Department subpoena process.
4. Unless prohibited by applicable law, ALPR data may be reviewed in accordance with the following criteria and exceptions:
    a. By a Department employee conducting an official investigation;
    b. By members of the City Attorney's Office or Risk Management in connection with pending litigation;
    c. Pursuant to lawful process by those otherwise authorized to view evidence in a related case;
    d. With approval by the Chief of Police, members reviewing a critical incident, internal reviews investigation, use of force review, or other internal reviews (e.g. Commission on Police Practices, Privacy Advisory Board);
    e. The Chief of Police has the discretion to allow the viewing or release of recorded files if they determine it is in the best interest of the Department. When appropriate, every effort is made to notify involved employees prior to release;
    f. As part of Department approved training;
    g. Subject to the provisions of this policy, the Chief of Police or the Executive Assistant Chief of Police has the discretion to prohibit the review of any recordings by Department employees if it is in the best interest of the Department or the City of San Diego.

MAINTENANCE

The San Diego Police Department shall maintain robust security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.

Surveillance Use Policy

Smart Streetlights
San Diego Police Department

PURPOSE

The primary purpose of Smart Streetlights is to facilitate the investigation of violent crimes, and traffic offenses that result in the loss of life, significant destruction of property, and erode the public safety of community members.

USE

Any integrations with additional technologies, such as facial recognition, or gunshot detection shall come to City Council for public review and approval, in accordance with the Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance, section 210.0103. Any modifications to this Policy must come to the City Council for public review and approval, in accordance with the TRUST Ordinance, section 210.0103. If Department Policy or Procedure conflicts with this Surveillance Use Policy, the Surveillance Use Policy will control.

The San Diego Police Department will use video evidence, along with data and information from authorized technologies embedded within Smart Streetlights, to conduct felony criminal investigations against persons and property, enhance responses to critical incidents and public threats, safeguard the lives of community members by using this technology to locate at-risk missing persons (including responding to Amber and Silver Alerts) and protect assets and resources of the City of San Diego.

Department Procedures associated with the use of Smart Streetlights are:

- Department members shall comply with Department Procedure (DP) 3.33 Smart Streetlights System and are subject to discipline for violations thereof, in accordance with City and Department rules and regulations.
- ~~DP 3.33 Smart Streetlight System~~
- DP 1.51 Automatic License Plate Recognition (ALPR)
- DP 3.02 Property and Evidence

The following uses are expressly prohibited:

a. Harassment or Intimidation: It is a violation of this Policy to use the Smart Streetlights system to harass and/or intimidate any individual or group.
b. Discrimination: It is a violation of this Policy to seek, submit, or retain Smart Streetlights data about individuals, or an organization, based solely on their religious beliefs, political affiliation, race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other classification protected by law.
c. Personal Use: It is a violation of this Policy to use the Smart Streetlights system for any personal purpose.

DATA COLLECTION

Smart Streetlight technology uses cameras to capture and store images from public spaces, where persons do not have a reasonable expectation of privacy. All videos gathered by the Smart Streetlights are for the official use of this department.

As Smart Streetlights are deployed, each camera will have privacy screens to mitigate private property recordings. The Smart Streetlights will be positioned to optimize collection of videos from public places to minimize collection of videos from places where an expectation of privacy exists or places exposed to view (e.g., parking lot of a shop or business).

Additional data points such as vehicle, bicycle, pedestrian counts, and the direction of their travel, as well as stationary vehicle detection, could be collected to optimize traffic control, pedestrian safety, and bicycle lane planning to further enhance public safety however, under the terms of the contract being considered these capabilities are not being considered.

Data collected by embedded technology, like ALPR, will be discussed in detail on specific use policies and procedures for this surveillance technology, see DP 1.51.

DATA ACCESS

Personnel authorized to use Smart Streetlights equipment or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. ~~Such personnel shall be limited to designated captains, lieutenants, sergeants, officers, detectives, and police department personnel unless otherwise authorized.~~ Authorized users include personnel listed in Department Procedure 3.33. Access will also be granted to supervisory staff of authorized users, (i.e., sergeants, lieutenants, captains) to ensure authorized users are complying with authorized usage, as well as Crime Analysts (backgrounded civilian non-sworn Department members) who enhance our investigations.

Authorized users under investigation for misconduct or criminal actions shall have their Smart Streetlights access revoked for the duration of the investigation and shall not have access restored until they have been cleared of wrongdoing.

~~Refer to DP 3.33, Smart Streetlight Systems, for additional details.~~

DATA PROTECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment, selecting, and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. 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

Department Procedure 3.33 mandates videos collected by Smart Streetlights shall be stored in a secured law enforcement facility with multiple layers of physical security and security protection. Encryption, firewalls, authentication, and other reasonable security measures shall be utilized to protect digital evidence from Smart Streetlights.

All Smart Streetlights videos downloaded from a video management solution to a mobile workstation or to digital evidence storage like Axon evidence shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time. Only those employees of the San Diego Police Department working in an investigative or enforcement function, and authorized by the Chief of Police, shall access Smart Streetlights videos.

DATA RETENTION

All Smart Streetlights videos collected and stored on this technology platform shall be purged no later than 15 days from the date it was collected, unless the video was determined to be evidence, downloaded, and stored pursuant to DP 3.02. The vendor shall confirm monthly in writing the deletion of City of San Diego data from their systems.

PUBLIC ACCESS

DP 3.33 provides detailed information related to the release of video images from Smart Streetlights, including their availability to members of the public via the California Public Records Act process, and by criminal defendants utilizing the discovery process as detailed in California's Evidence Code.

THIRD PARTY DATA SHARING

~~Smart Streetlights videos may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, which includes enhancing criminal investigation and prosecution as allowed by law. See DP 3.33 for additional details related to the use and release of evidence from Smart Streetlights.~~

- Smart Streetlights data shall never be shared with Immigration and Customs Enforcement or Border Patrol for the purpose of enforcing immigration laws.
- Smart Streetlights data shall never be released to aid in the prosecution of an individual for providing, obtaining, or assisting in the provision or obtention of an abortion or any reproductive care.
- Smart Streetlights data shall never be shared with any federal taskforces which involve in any manner the investigation or prosecution of federal crimes, for conduct which is permitted under California law.
- No Smart Streetlights data shall be released to outside sources, except the San Diego City Attorney and San Diego District Attorney in accordance with legal proceedings or California law enforcement agencies for the express purpose of investigating cross-jurisdictional Part I crimes, until the adoption of a third-party data sharing use policy by the City Council.
- Nothing in this Policy should be interpreted as limiting the use of collected data for legitimate purposes by prosecutors or others legally permitted to receive evidence under law.

TRAINING

Training for the operation of Smart Streetlights technology utilized by the San Diego Police Department shall be provided by Police personnel or subject matter experts approved by the Department. All employees who utilize Smart Streetlights technology shall be provided a copy of this Surveillance Use Policy, along with instruction of the constitutional protections and case law requirements associated with its lawful use.

AUDITING AND OVERSIGHT

Personnel who are authorized to have access to the system shall be designated in writing and the designation shall ensure that their access to and use of the videos complies with the Surveillance Ordinance and applicable Department procedures referenced in this Surveillance Use Policy.

A log shall be maintained that records when access to Smart Streetlights videos are requested. This shall include the date, time, data record accessed, and staff member involved. The log shall be available for presentation for all required internal and external audits, and oversight will be maintained by the system Program Manager or their designee.

1. All evidence collected from the Smart Streetlights is considered an investigative record for the Department and is for official use only.
2. Requests for recorded video images from the public or the media shall be processed in the same manner as requests for Department public records.
3. Record videos images that are the subject of a court order or subpoena shall be processed in accordance with the established Department subpoena process.
4. Unless prohibited by applicable law, recorded files may be reviewed in accordance with the following criteria and exceptions:
    a. By a Department employee conducting an official investigation;
    b. By members of the City Attorney's Office or Risk Management in connection with pending litigation;
    c. Pursuant to lawful process or by court personnel otherwise authorized to view evidence in a related case;
    d. With approval by the Chief of Police, members reviewing a critical incident, internal reviews investigation, use of force review, or other internal reviews (e.g. Commission on Police Practices, Privacy Advisory Board);
    e. The Chief of Police has the discretion to allow the viewing or release of recorded files if they determine it is in the best interest of the Department. When appropriate, every effort is made to notify involved employees prior to release;
    f. As part of Department approved training;
    g. An officer involved in the intentional discharge of a firearm, an incident where any party sustains great bodily injury, or an in custody death shall not review recorded footage from Smart Streetlights unless approved by the Chief of Police or the Executive Assistant Chief of Police;
    h. Subject to the provisions of this policy, the Chief of Police or the Executive Assistant Chief of Police has the discretion to prohibit the review of any recordings by Department employees if it is in the best interest of the Department or the City of San Diego.

~~Any misuse of this technology shall result in disciplinary actions as outlined in DP 3.33.~~

MAINTENANCE

The San Diego Police Department shall maintain robust security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect Smart Streetlights information from unauthorized access, destruction, use, modification, or disclosure.