

City of San José

Data Usage Protocol (DUP) for Automated License Plate Reader (ALPR) Technology

Owning department(s): San José Police Department (SJPD)
Department owner: Deputy Chief, Executive Officer

1) Purpose

Automated License Plate Readers (ALPRs) use high speed cameras to photograph vehicle license plates. The purpose of ALPR cameras is to improve criminal investigations¹ and deter crime in the surrounding area.² This Data Usage Protocol (DUP) defines for the City of San José's (hereafter referred to as "City") Police Department ("hereafter referred to as "Department"):

1. Authorized usage of ALPR technology that complies with State and local laws;
2. Annual reporting requirements on ALPR usage; and
3. An ongoing avenue for public feedback on ALPR usage.

This DUP is also meant to ensure that San Jose Police Department's use of Automated License Plate Recognition (ALPR) technology complies with all applicable federal, state, and local laws. For the purposes of California law, this document serves as the "usage and privacy policy" as required by California Civil Code Sections 1798.29 and 1798.82.

2) Authorized Uses:

The Department shall use ALPR technology with the goal of reducing serious crime and traffic incidents in the long term. ALPR is meant to act as a deterrent for crime and dangerous driving in a neighborhood, and to support police in criminal investigations. ALPR vendors may only use the data if authorized by the City to act on behalf of the City. The Department and authorized vendors may utilize ALPR technology and any data generated only to do the following:

1. Use in conjunction with any patrol or investigative function in response to the investigation of felony or misdemeanor crimes;
2. Locate at-risk missing persons (including responding to Amber and Silver Alerts);

¹ Koper, Christopher S., and Cynthia Lum. "The impacts of large-scale license plate reader deployment on criminal investigations." *Police Quarterly* 22.3 (2019): 305-329 – <https://journals.sagepub.com/doi/abs/10.1177/1098611119828039>

² Koper, Christopher S., Bruce G. Taylor, and Daniel J. Woods. "A randomized test of initial and residual deterrence from directed patrols and use of license plate readers at crime hot spots." *Journal of Experimental Criminology* 9.2 (2013): 213-244 – <https://link.springer.com/article/10.1007/s11292-012-9170-z>

3. Support local and State safety departments in the identification of vehicles associated with criminal investigations. Further detail on permissible sharing and coordination with safety departments is detailed in the “Data Sharing” section below; and
4. Automatically initiate investigation for traffic intersection infractions through a device (e.g., red-light violations) if SJPD follows the requirements outlined in California Vehicle Code 21455.5,³ including providing notice of automated enforcement within 200 feet of the intersection.

3) Prohibited Uses:

ALPR technology will not be used for the following purposes:

1. Collect data that is not within the public view. This includes any data not readily visible from a public area or public property;
2. Monitor individual or group activities legally allowed in the State of California and/or protected by the First Amendment to the United States Constitution;
3. Share with immigration authorities or use in the investigation of any matter related to immigration status of an individual;
4. Engage in automated citations or other automated enforcement without manual review from SJPD staff; and
5. Sell any data generated by ALPR to any entity.

4) Operational Procedures

The ALPR system(s) and their associated database(s) shall only be used for official law enforcement purposes listed in the “Authorized Uses” section. Additionally:

1. No member of the Department shall operate, utilize and/or search ALPR systems and their associated equipment/database(s) without first completing Department-approved training and only if the operation, utilization, or searching complies with SJPD’s need to know/right to know protocols defined in SJPD Duty Manual section C2000 on criminal records and information;⁴
2. Once an alert is received, the officer will make every effort to visually confirm that the captured license plate from the ALPR system matches the license plate of the observed vehicle;
3. In all instances, before any action is taken based solely upon an ALPR alert, the officer will make every effort to verify the alert is still valid through the California Law Enforcement Telecommunications System (CLETS). Officers will not take any action that restricts the freedom of any individual based solely upon an ALPR alert until an attempt at verification has been made;
4. If the reason for an ALPR alert pertains to a wanted person associated with a vehicle, officers should attempt to visually inspect the occupant(s) of the vehicle to determine if he/she matches the description of the wanted individual. Absent this verification, officers must have a separate legal justification to conduct a vehicle stop;

³ California Vehicle Code “Offenses Relating to Traffic Devices” - https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=21455.5.&nodeTreePath=15.2.3&lawCode=VEH

⁴ See SJPD Duty Manual - <http://www.sjpd.org/records/dutymanual.asp>

5. Designation of vehicles into “hot lists”⁵ shall be the sole responsibility of the assigned investigating officer or his/her designee. Vehicle’s cannot be entered into “hot lists” without a lieutenant’s approval. It will be the arresting/investigating officer’s responsibility to ensure timely entry/removal of license plates into/out of the designated “hot lists”.
6. To the best of the system administrator or his/her designee’s ability, hot lists managed by an external source (e.g., the Stolen Vehicle System) will be synchronized with the external hot list at all times. In the event of a loss of connection to external hot lists, the ALPR system administrator or his/her designee shall synchronize with external hot-lists upon reconnection;
7. Protocols shall be established to ensure timely notification is made to the system administrator to indicate and record when a “hot list” ALPR license plate capture is made and the ultimate disposition of the specific enforcement action;⁶ and
8. All vehicles entered into a departmental “hot list” will contain the following information:
 - a. Name, badge number and assignment of department member entering the information (e.g., Officer Smith #1234, Robbery Unit)
 - b. Associated case number(s)
 - c. Short synopsis describing the reason for the vehicle/occupant database entry. This should include the presumed crime or crimes relevant to this investigation. If no crime is relevant, state the other purpose (e.g., Amber alert)

5) Data Collection

ALPR utilizes high speed cameras angled to capture digital images of vehicle license plates on public roads and private property visible from a public road (e.g., a driveway). The cameras are trained on the license plate of a vehicle and rarely capture the image of a person. The cameras do not identify an individual or group based on physical characteristics such as skin-tone, body shape, or facial features.

An example image captured from an ALPR camera is provided in Figure 1. While the ALPR camera is angled to capture license plate information, it may collect additional information visible in the image, including car make/model, and other distinguishing characteristics of the vehicle (e.g., bumper sticker(s), after market wheels, etc.).

ALPR cameras may be placed in a fixed location, such as on a street light pole, or in a roaming location, such as on a police vehicle. The technology will record the date and time the image was captured as well as the location of the camera. The exact location of a vehicle is not tracked, but can be inferred based on the location of the camera at the time of the photograph.

⁵ License plate(s) associated with vehicles of interest from an associated database, including, but not limited to: California Law Enforcement Telecommunications System (CLETS), National Crime Information Center (NCIC), Be on the Lookout notices (BOLOs), and Department databases

⁶ An example notification would be: “Hot list 211A vehicle alerted at Curtner/Monterey, observed at Curtner/Malone. Vehicle stopped, driver arrested for 211”



Figure 1: Police vehicle with an Automated License Plate Reader mounted on its roof, and an example picture from the ALPR camera (top-left). This ALPR picture identifies 1) the license plate, 2) the time and location of the car, and 3) other information captured in the photograph, including vehicle color, make, and model. Source: Pasadena, CA Police Department.

<https://www.pasadenanow.com/main/city-council-to-consider-purchasing-more-automatic-license-plate-readers>

6) Notice

Notice that the City of San José is using ALPR technology will be posted as signage at major vehicle entrances into the city and exits from the city, and at “designated intersections” within the city to notify residents that ALPR cameras may be present in their area.

“Designated intersections” refers to locations near where ALPR technology is being utilized. The signs will contain notice that ALPR technology is in use and will direct the reader to where they can get more information about the ALPR program and policies. Notice and additional detail, including this Data Usage Protocol, will be available on the City website.

7) Retention and Minimization

Data collected from ALPR technology will be retained for one year. Once the retention period has expired, the record shall be purged entirely from all active and backup systems unless the data is related to an active investigation of a crime not listed in the “Prohibited Uses” section.

Data associated with a criminal investigation may be stored for longer on an electronic storage device or printed and retained in accordance with applicable state and federal evidentiary laws, to include retaining the data through the adjudication of a case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations.

8) Access and Accuracy

Raw ALPR data, including photographs, license plates, location, and associated hot list data will not be available for public access unless required pursuant to city, state, or federal law, or a court order. Aggregated data on the ALPR technology, including performance metrics on the accuracy of the technology, will be made available annually in the Annual Data Usage Report. More details on the Annual Data Usage Report can be found in the “Annual Data Usage Report requirements” section below. The City may release more aggregated data periodically at its discretion.

9) Accountability

All Department members authorized to use or access ALPR technology or data shall be accountable for knowledge of this protocol. See “Training” section for definition of authorized personnel.

All access to the system shall be logged, and the Department will maintain an audit trail of requested and accessed information, including the purpose of the query. Periodic, random audits shall be conducted by a unit other than Crime Data Intelligence Center (CDIC) at the direction of the Deputy Chief, Executive Officer to ensure and evaluate compliance with system requirements and with the provisions of this protocol and applicable law. Audit trails shall be maintained by the Department for a minimum of two (2) years. Additional audits or reviews may be triggered at the direction of the City Council or Digital Privacy Officer (DPO), consistent with state law and authorized access to information.

If a Department member accesses or provides access to ALPR information, the Department member shall do the following:

1. Maintain a record of the access that includes the following information:
 - a. Date/Time the Information was accessed
 - b. The license plate number or other data elements used to query the ALPR system
 - c. The name and department of the person who accessed the information
 - d. The purpose for accessing the information, including the presumed crime or crimes relevant to this investigation. If no crime is relevant, state the other purpose (e.g., Amber alert)
2. ALPR information may only be used for authorized purposes as specified in this protocol in accordance with California Civil Code section 1798.90.51(b).

10) Sharing

The City does not share ALPR data with any contracted, commercial, or private entity. The provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR information (see CA Civil Code 1798.90.55.(b)).

Information gathered or collected, and records retained by the City will not be:

1. Sold, published, exchanged, or disclosed for commercial purposes;

Data Usage Protocol (DUP) for Automated License Plate Reader (ALPR) Technology
UPDATED as of August 22, 2022

2. Disclosed or published without authorization; or
3. Disseminated to persons not authorized to access or use the information.

The City shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law. The City may agree to share access to its ALPR database by law enforcement agencies within the State of California on an agency-by-agency basis if an agreement is put into place.

The data will not be shared beyond the approved agencies. All agencies must request SJPD ALPR data directly from SJPD (e.g., if SJPD shares ALPR data with Santa Clara PD, Sunnyvale PD must request SJPD data through SJPD rather than Santa Clara). The requesting agency may only access the data for an authorized purpose as noted in this protocol.

Logs will be generated every time an approved law enforcement agency accesses data from SJPD's ALPR system, which will include:

- a. Date/Time the Information was accessed
- b. The license plate number or other data elements used to query the ALPR system
- c. The name and law enforcement agency of the person who accessed the information
- d. The purpose for accessing the information

11) Equity and Community Engagement

The City will make a reasonable effort to identify and mitigate any inequity inherent in the ALPR technology and its implementation. Members of the public may submit any concerns via the public comment feature at sanjoseca.gov/digitalprivacy. Comments may also be submitted by emailing digitalprivacy@sanjoseca.gov or mailing the Digital Privacy Officer at 200 E Santa Clara St. San Jose CA 95113, 11th Floor. ALPR implementations can impact certain populations more than others. The City of San Jose is cognizant of that concern and will field potential complaints when submitted by emailing: digitalprivacy@sanjoseca.gov. After receiving a complaint, the City will perform an investigation and determine a corrective action plan, if necessary.

12) Storage and Security

Data collected by ALPR technology shall be stored in a secured police facility or secured third-party hosting environment. With the exception of audits, access to the raw data (images of vehicles and license plates) shall be limited to law enforcement staff with a legitimate need and right to access the information. The Department will utilize reasonable physical, technological, administrative, procedural, and personnel security measures to prevent unauthorized access to ALPR data. Authorized sworn personnel or authorized civilian personnel (such as a crime analyst) shall have general user access to the SJPD ALPR database, as appropriate, to query information. See "Training" section for definition of "authorized personnel". Entities authorized to audit the ALPR system (see "Accountability" section for who can authorize) do not need to be a part of the Department to access the database.

Data Usage Protocol (DUP) for Automated License Plate Reader (ALPR) Technology
UPDATED as of August 22, 2022

Sworn personnel or authorized civilian personnel as approved by the Deputy Chief, Executive Officer, or his/her designee shall have administrative user access to the SJPD ALPR database, as appropriate, to control:

1. The information to which a particular group or class of users can have access based on the group or class;
2. The information a class of users can access, and/or data being utilized in specific investigations;
3. Sharing capabilities with other law enforcement agencies; and
4. Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the data or equipment.

The Bureau of Technical Services Systems Development Unit may provide ALPR technical support for the Criminal Data Intelligence Center (CDIC). The CDIC shall ensure compliance with this protocol. The custodian of ALPR data for purposes of this protocol shall be the Deputy Chief, Executive Officer or his/her designee.

In the event of a confirmed data breach where personal information such as license plate numbers or photographs have been accessed by an unauthorized party, the Department will follow the City of San José's Incident Response Plan. This security protocol and further security details are overseen by the City's Cybersecurity Office.

13) Training

Except for audits, only authorized personnel, meaning Department personnel trained in the use of ALPR technology, including its privacy and civil liberties protections, shall be allowed access to ALPR data. Training shall consist of:

1. Legal authorities related to the use of ALPR data and technology;
2. Current Department Data Usage Protocol regarding authorized use of ALPR technology;
3. Technical, physical, administrative, and procedural measures to protect the security of ALPR data against unauthorized access or use; and
4. Practical exercises in the use of ALPR technology.

14) Annual Data Usage Report requirements

To provide the City and the public with ongoing reporting on the usage and accuracy of the ALPR technology, the following information will be required in an Annual Data Usage Report submitted every year to the Digital Privacy Officer (DPO) no later than March 1st and covers the previous calendar year (January 1st – December 31st). In the year this Data Usage Protocol goes into effect, the Department is only required to report on the period from the date the Data Usage Protocol goes into effect until the end of the calendar year.⁷ The Digital Privacy Officer will release the report to the public once private, confidential, and otherwise sensitive information is removed. The DPO shall release the report within 90 days of receiving it from the department, unless additional time is required to remove private, confidential, and sensitive information. If

⁷ If this Data Usage Protocol is passed after September 30th, the first Annual Data Usage Report will not be required until the following year, which will cover usage from the date the Data Usage Protocol goes into effect to December 31st of the following year

Data Usage Protocol (DUP) for Automated License Plate Reader (ALPR) Technology

UPDATED as of August 22, 2022

the DPO needs additional time, they shall provide a notice of extension to the public via the Digital Privacy webpage.⁸

1. Summary of the project and updates since the prior year, including detail on value to the department
2. Plans for future years, including any planned expansion of project or shift in data usage
3. Reporting metrics on ALPR usage and accuracy including:
 - a. **# of reads by location** – the Department will either:
 - i. Report directly the number of reads by location; or
 - ii. Provide the Digital Privacy Officer (DPO) with access to the ALPR reads database, including the latitude and longitude of each read, from which the DPO can report by location as needed.
 - b. **# of hits by location** – Similar to the # of reads by location, the Department will either:
 - i. Report directly the number of hits by location; or
 - ii. Provide the DPO with access to the ALPR reads database, including the latitude and longitude of each read and if the read was a hit, from which the DPO can report by location as needed.
 - c. **Records accessed by SJPD** – the Department will report on the number of records accessed in accordance with the Accountability section of this Protocol.
 - d. **Accuracy of accessed records** – the Department will report on the accuracy of the implemented ALPR technology as requested by Council and the DPO

⁸ Link to the digital privacy webpage: <https://www.sanjoseca.gov/your-government/departments-offices/information-technology/digital-privacy>