Surveillance Use Policy for fixed Automated License Plate Recognition (ALPR) Technology

In accordance with Palo Alto Municipal Code Section PAMC 2.30.680(d), the Surveillance Use Policy for the Police Department's use of fixed ALPR technology is as follows:

1. **Intended Purpose.** The technology is used by the Palo Alto Police Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including but not limited to identifying stolen or wanted vehicles, stolen license plates and missing persons, suspect interdiction and stolen property recovery.

2. **Authorized Uses.** Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this Policy.

   The following uses of the ALPR system are specifically 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. Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
   c. First Amendment Rights. It is a violation of this policy to use the LPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights of any person.
   d. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, 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).

3. **Information Collected.** A fixed ALPR system captures the date, time, location, license plate (state, partial, paper, and no plate), and vehicle characteristics (make, model, type, and color) of passing vehicles. using the Palo Alto Police Department's ALPR's system and the vendor's vehicle identification technology.

4. **Safeguards.** All data will be closely safeguarded and protected by both procedural and technological means. The Palo Alto Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):
   a. All ALPR data shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

b. Persons approved to access ALPR data under this policy are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation
c. Such ALPR data may only be released to other authorized and verified local enforcement officials and agencies for legitimate law enforcement purposes.
d. Every ALPR system inquiry must be documented by either the associated case number or incident number, and lawful reason for the inquiry.

5. **Retention.** The City's ALPR vendor, Flock Safety, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data centers. Flock Safety will purge the data 30 days after collection; however, this will not preclude Palo Alto Police Department from maintaining any relevant vehicle data obtained from the system after that period if it has become, or it is reasonable to believe it will become, evidence in a specific criminal investigation or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

   Information gathered or collected, and records retained by Flock Safety cameras will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

6. **Access by non-City Entities.** The ALPR data may be shared only with other local law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise required by law, and as provided below:
   a. Requests
      i. A law enforcement agency may make a written request for specific data, including the name of the agency and the intended official law enforcement purpose for access
      ii. The request shall be reviewed by the Chief of Police or the authorized designee and approved before access is granted
      iii. The approved request is retained on file
      iv. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed by the Department's custodian of records and fulfilled only as required by law.
   b. Memorandaphilip of Understanding
      i. Access to searchable data by other local law enforcement agencies shall only be granted pursuant to an MOU with that specific agency
      ii. Such MOU will provide that access will only be used for legitimate law enforcement or public safety purposes
   c. The Chief of Police or the authorized designee will consider the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq), before approving the access to ALPR data. The Palo Alto Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement.

7. **<u>Compliance Procedures.</u>** The Investigative Services Captain (or other police administrator as designated by the Police Chief) shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):
    a. Only properly trained sworn officers, crime analysts, and police staff are allowed access to the ALPR system or to collect ALPR information.
    b. Ensuring that training requirements are completed for authorized users.
    c. ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.
    d. Ensuring that procedures are followed for system operators and to maintain records of in compliance with Civil Code § 1798.90.52.
    e. The title and name of the current designee in overseeing the ALPR operation is maintained. Continually working with the Custodian of Records on the retention and destruction of ALPR data as required.
    f. Ensuring this policy and related procedures are conspicuously posted on the Department's dedicated ALPR website.

    It is the responsibility of the Investigative Services Captain (or other police administrator as designated by the Police Chief) to ensure that an audit is conducted of ALPR detection inquiries at least once during each calendar year. The Department will audit a sampling of the ALPR system utilization from the prior 12-month period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by department employees during the preceding six-month period and determine if each inquiry meets the requirements established by policy. This audit shall take the form of an internal Department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be filed and retained by the Department.