DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: XX
Coordinator: Information Technology Unit

This policy provides guidance for the capture, storage and use of digital data obtained through the use of ALPR technology while recognizing the established privacy rights of the public.

Definitions

(a) **Automated License Plate Reader (ALPR):** A device that uses cameras and computer technology to compare digital images of vehicle license plates to lists of known information of interest.

(b) **Hot List:** A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to the Stolen Vehicle System (SVS), NCIC, and local BOLO alerts.

(c) **Hit:** Alert from the ALPR system that a scanned license plate may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person or domestic violence protective order.

A. Description of the Technology: *Information describing the surveillance technology and how it works.*

OPD uses Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images. There are two components to the ALPR system:

1. Automated License Plate Readers: Device components include cameras which can be attached to vehicles or fixed objects and a vehicle-based computer that processes the photographs and compares the data against California Department of Justice (CA DOJ) hot-lists. Data are transmitted for comparison (the hot lists are downloaded to the vehicle at the start of the patrol shift and then compared from that list). Authorized personnel can also manually enter license plates to internal OPD generated hot-lists only accessible to personnel authorized to access the OPD ALPR system.

2. ALPR Database: A central repository stores data collected and transmitted by the Automated License Plate Readers.

B. Purpose of the Technology

ALPR technology works by automatically and indiscriminately scanning all license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters against Hot Lists, and stores the characters along with the date, time, and location where the photograph was taken. This process allows for two functions by ALPR:

1. Immediate (real time) comparison of the license plate characters against Hot Lists listing vehicles that are stolen or sought in connection with a crime and/or with OPD-generated internal lists.

2. Storage of the license plate characters – along with the date, time, and location where the photography was taken – in a database that is accessible to enforcement agencies with authorized access (as defined in "Authorized Use" below) for investigative query purposes.

C. Authorized Uses: *The specific uses that are authorized, and the rules and processes required prior to such use.*

1. **Authorized Users**

Personnel authorized to use ALPR equipment or access information collected through the use of such equipment shall be specifically trained in such technology. Sworn personnel, Police Service Technicians, or other authorized Department personnel may use the technology. Authorized users other than sworn personnel or police services technicians (PST) must be designated by the Chief of Police or designee.

2. Authorized use

(A) **Real-Time Identification**: The officer shall verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before possibly taking enforcement action that is based solely on an ALPR alert.

Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle.

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been fully validated, by visually verifying that the license plate characters on the vehicle match those in the database, and that the make, model, color and all other known identifying characteristics likewise match.

(1) **Hot Lists**. The Department shall only use the following hot lists: Stolen Vehicle System ("SVS"), National Crime Information Center ("NCIC") lists, CA DOJ lists, Amber and Silver alerts, and custom BOLO lists pertaining solely to missing or at-risk persons, witness locates, and violent crime investigation. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Department's LPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's LPR system will not have access to real time data. Occasionally, there may be errors in the LPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

(2) Department members will clear all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action on a computer generated spreadsheet that shall include at minimum a) the Department member's name that responded to the alert, b) the justification for responding to the alert, c) the related case number, d) the disposition code, e) time and date of the response, and d) and any known next steps or follow up (e.g. forwarding case to District Attorney, alerting owner to recovered stolen vehicle).

(B) **Database Investigative Queries**: Historical searches of scanned plates is permissible solely for missing or at-risk persons, witness locates, violent crime investigation, and in response to any subpoena, warrant, or other court order.

For each query, the Department shall record (1) the date and time the information is accessed, (2) the license plate number or other data elements used to query the ALPR system, (3) the username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated, and (4) the purpose for accessing the information. These records shall be attached to the annual report required by O.M.C. 9.64 et seq.

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

(4) General Hot Lists (such as SVS and NCIC) will be automatically downloaded into the ALP system a minimum of once a day with the most current data overwriting the old data.

(5) All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. All entries shall be approved by the ALPR Administrator (or his/her designee) before initial entry within the ALPR system. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles of interest that might have been associated with criminal activity.

All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:

- Entering Department member's name
- Related case number
- Justification for entering the plate and/or other identifying information onto the Hot List.
- Date and time of entry

3. Restrictions on Use

Permitted/Impermissible Uses. The ALPR system, and all data collected, is the property of the Oakland Police Department. Department personnel may only access and use the ALPR system consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

(1) Invasion of Privacy: 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).

(2) Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.

(3) Use Based on a Protected Characteristic. It is a violation of this policy to use the LPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.

(4) 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.

(5) 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.

Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose (Civil Code §798.90.51.; Civil Code § 1798.90.53).

a. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

b. No ALPR operator may access department, state or federal data unless otherwise authorized to do so pursuant to Section E "Data Access" below.

c. Accessing data collected by ALPR requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a state or federal statute, applicable case law, or a court order. A need to know is a compelling reason to request information such as involvement in an active investigation.

D. Data Collection: *The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data.*

ALPR technology works by automatically scanning license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters (as well as vehicle attributes such as vehicle color or make and model with some ALPR systems) against specific databases, and stores the characters along with the date, time, and location where the photograph was taken, in a database.

E. Data Access: *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.*

Department sworn personnel, police service technicians, or other authorized Department personnel may use the technology. Authorized users other than sworn personnel or police services technicians (PST) must be designated by the Chief of Police or designee.
Data may not be shared with out of state or federal agencies, per California law.

The Oakland Police Department does not permit the sharing of ALPR data gathered by the city or its contractors/subcontractors for purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

All data and images gathered by the ALPR are for the official use of this department. Some information may not be disclosable to the general public. Investigatory records are not generally disclosable in response to a public records request. Non-investigatory records shall be disclosed in response to a public records request.

F. Data Protection: *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms.*

All data shall be safeguarded and protected by both procedural and technological means. OPD shall observe the following safeguards regarding access to and use of stored data. (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR server data shall be accessible only through a login/password-protected system capable of documenting all access of information by username, license number or other data elements used in the search, name, date, time and purpose. (Civil Code § 1798.90.52).

2. Data will be transferred from vehicles to the designated storage per the automated ALPR technology data transfer protocol.

G. Data Retention: *The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to keep information beyond that period.*

All ALPR data uploaded to the server shall be purged from the server at the point of 30 days from initial upload. ALPR information may be retained outside this retention limit solely for the following purposes:

1. Active Criminal Investigations
2. Missing or at-risk Persons Investigations

4. Investigations from other law enforcement or prosecutorial agencies where there is a legal obligation to retain information.

H. Public Access: *how collected information can be accessed or used by members of the public, including criminal defendants.*

Requests for ALPR information by non-law enforcement or non-prosecutorial agencies will be processed in accordance with Civil Code § 1798.90.55, Government Code §6253 et seq, this policy, and applicable case law and court orders.

I. Third Party Data Sharing: *If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.*

ALPR server data may be shared only as otherwise permitted by law and this policy. All data and images gathered by the ALPR are for the official use of this Department.

OPD personnel may share ALPR server data when there is a legal obligation to do so, such as a subpoena, court order or warrant to share such information, such as the following:

- a District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- a Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with applicable California criminal discovery laws;
- California law enforcement agencies as part of a formal criminal or administrative investigation;
- a party to civil litigation, or other third parties, in response to a valid court order only.

When there is no legal obligation to provide the requested data, requests for ALPR server data from other California law enforcement agencies shall be made in writing and may only be approved by the BOS deputy director or designee per the protocol below. These requests shall be maintained in a secure folder so that information about these requests can be shared in required annual reports with the PAC. Server access shall be restricted only to authorized OPD personnel who will extract the required information and forward it to the requester.

1. The requesting party shall have a right to know, and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, case law, or sworn officer status. A need to know is a compelling reason to request information such as direct involvement in an investigation.
2. The Department shall record the requesting party’s name and document the right and need to know the requested information.

3. The Department shall record whether the request was honored or denied, the reason for such action, and the name of the Department officer that processed the request.

J. Training

The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

The Training Section shall ensure that members receive department-approved training for those authorized to use or access the ALPR system and shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

Training requirements for employees shall include the following:

- Applicable federal and state law
- Applicable policy
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

K. Auditing and Oversight

The mechanisms to ensure that the Surveillance Use policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited. It is the responsibility of the Department under this policy to actively pursue software and hardware upgrades that are needed to maintain full compliance with Section K of the use policy.

The records of Database Investigatory Queries, Third Party Data Sharing, and Hot List entries shall be incorporated into the annual report required by O.M.C. 9.64 et seq.

ALPR system audits shall be conducted annually to ensure proper system functionality and that personnel are using the system according to policy rules via sample audits, reviews of training records

L. Maintenance

The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

1. ALPR Administration: All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the BOS.

2. ALPR Administrator: The BOS Deputy Director shall be the administrator of the ALPR program and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code §1798.90.5 et seq. The BOS Deputy Director is responsible for ensuring systems and processes are in place for the proper collection, and retention of ALPR data.

3. ALPR Coordinator: The title of the official custodian of the ALPR system is the ALPR Coordinator.

4. Monitoring and Reporting: The Oakland Police Department will ensure that the system is remains functional according to its intended use and monitor its use of ALPR technology to ensure the proper
functionality of the system as defined in the policy guidelines of this document, including required audits, training, and data access records.

5. The ALPR Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report pursuant to OMC 9.64 (Oakland Surveillance Technology
Ordinance).

By Order of

Leronne Armstrong Chief of Police Date Signed: