DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: XX
Coordinator: Information Technology Unit

The Oakland Police Department (OPD) strives to use technology that promotes accountability and transparency. 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.

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) hotlists. D~~; d~~ata is transmitted for comparison (the hotlists 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 hotlists 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 scanning license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters against California Department of Justice (CA DOJ) ~~specific~~ databases, and stores the characters along with the date, time, and location where the photograph was taken, in a database. This process allows for two functions by ALPR:

1. Immediate (real time) comparison of the license plate characters against CA DOJ databases 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 Use: *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. Restrictions on Use

Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51~~.~~; Civil Code § 1798.90.53). Authorized purposes consist only of queries related to criminal investigations, administrative investigations, missing persons cases, or other situations where there is a legal obligation to provide information related to an investigation. Any situation outside of these categories requires approval from a commander at the rank of Deputy Chief, Deputy Director, or higher.

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 D "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.*

ALPR server data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

All data and images gathered by the ALPR are for the official use of this department. Because such data contains investigatory and/or confidential information, it is not open to public review.

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

All data will be safeguarded and protected by both procedural and technological means. OPD will 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). In the event that the system cannot perform these functions, OPD personnel shall explain in writing to the City's Chief Privacy Officer within seven days of receiving notice of the diminished functionality.

2. Members approved to access ALPR data under these guidelines are permitted to access the data for law enforcement purposes only, as set forth above in Section B.2(1)(c) "Restrictions on Use."

3. Data will be transferred from vehicles to the designated storage per the ~~with~~ 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 retain information beyond that period.

All ALPR data uploaded to the server shall be purged from the server at the point of 365 days~~twelve months~~ from initial upload. ALPR information may be retained outside the database for the following purposes:

1. Criminal Investigations
2. Administrative Investigations
3. Missing Persons Investigations
4. Investigations from other law enforcement or prosecutorial agencies where there is a legal obligation to provide information.

Any situation outside of these categories requires approval from a commander at the rank of Deputy Chief, Deputy Director, or higher.

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 as provided in Departmental General Order M-9.1, Public Records Access, in accordance with (Civil Code § 1798.90.55, Government Code § 6253 et seq., 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 with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. All data and images gathered by the ALPR are for the official use of this department. Personnel may also grant ALPR server access to law enforcement agencies with whom OPD has an MOU that allows data sharing. Because such data contains investigatory and/or confidential information, any requests for public records access or requests must go through the protocol as set forth in E., F, and H (above).

OPD personnel may share ALPR server data with other law enforcement or prosecutorial agencies when there is a legal obligation, such as a court mandate, to share such information.

Requests for ALPR server data, where there is not a legal obligation to provide the data, shall be made in writing and approved by the BOS Deputy Director or designee. 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.

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 recordkeeping 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.*

ALPR system audits shall be conducted annually by BOS to ensure proper system functionality and that personnel are using the system according to policy rules via sample audits, reviews of training records, and all requirements outlined in OMC 9.64 Section E "Data Protection" above explains that designated personnel will notify the City's Privacy Officer within seven days upon a finding that the ALPR system cannot fully produce system audits due to technical issues with the system.

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…. maintained according to 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.

   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 L. Armstrong
Chief of Police Date Signed: