

NUMBER: 24-001	Original Issue: May 15, 2024	Revised Date:	Effective Date: May 15, 2024
SUBJECT: Automated License Plate Readers (ALPR)			Pages: 5

I. PURPOSE

The purpose of this policy is to provide Warren Police Department officers guidance on the application and use of automated license plate readers (ALPR) along with the management of data and maintenance of ALPR equipment.

II. POLICY

ALPRs are used by the Warren Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, sex offenders, and missing persons. ALPRs may also be used for any other official law enforcement purpose; including, but not limited to, identifying suspects in crimes under investigation, apprehending fugitives, recovering stolen property, electronic surveillance, homeland security, and criminal interdiction. It is the intent of the Warren Police Department to ensure that the access and use of ALPR data is consistent with respect for individual's privacy, civil liberties, and the law. All officers will use ALPRs in accordance with the procedures and guidelines set forth, and all data captured will be used properly and responsibly.

III. DEFINITIONS

A. ALERT (AKA. "HIT")

A positive indication, by visual and/or audible signal, of a potential match between data on the "Hot List" and a license plate scanned by the ALPR system. An alert or hit is not conclusive confirmation that a license plate is wanted, and additional investigation is always warranted when an alert is indicated.

B. ALPR COORDINATOR

Designee of the Chief of Police who will conduct annual or more frequent auditing and reporting of ALPR use and effectiveness to the Chief of Police.

C. AUTOMATED LICENSE PLATE READER (ALPR)

A device that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest. ALPRs may be deployed in different configurations including fixed

(permanent or semi-permanent installation at a specific location) and mobile (attached to a vehicle or trailer). Both configurations operate in the same manner.

D. CUSTOM HOT LIST

License plates or vehicle descriptions that are derived from investigative leads that require manual input such as a WPD BOLO, stolen vehicles that have not yet been entered into LEADS, any vehicle involved in an active investigation, etc.

E. FIXED LOCATION ALPR

Fixed ALPR locations use cameras that are engineered to focus on the rear license plate of vehicles passing by the camera location. The camera images are sent by cellular data signal to an off-site server where the images are compared with license plates from the National Crime Information Center (NCIC) and local hot lists. License plates that match an NCIC entry or hot list trigger an alert to the user who is logged in to monitor the ALPR system. Although all plates are imaged, only the NCIC entered or hot list plates trigger an alert. The images of the license plates of vehicles passing by the camera are retained for no longer than 30 days.

F. HOT LIST

License plates associated with vehicles of interest from an associated database including, but not limited to, NCIC, Department of Motor Vehicles, local BOLOs, etc.

G. SCAN FILE

Data obtained by an ALPR of license plates within public view that were read by the device, including potential images of the plate and vehicle on which it was displayed, and information regarding the location of the fixed camera position at the time of the ALPR read. Information stored includes a photo of the registration plate showing the rear of the vehicle, a date and time stamp of when the registration plate was read by the ALPR, and a Global Positioning System (GPS) coordinate to identify the location the registration plate was read by the ALPR.

IV. ADMINISTRATION OF ALPR SYSTEM

The Criminal Investigations Division Commander is designated as the ALPR Coordinator and manages the operation of ALPR equipment and access to data.

V. ALPR OPERATION

Departmental use of ALPR is restricted to the purposes outlined below. Officers shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

- A. An ALPR shall only be used for official and legitimate law enforcement purposes.
- B. An ALPR may be used in conjunction with any official Warren Police investigation.
- C. While an ALPR may be used to capture license plates around any crime scene, homicides, shootings, and other major incidents, partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles as soon as practical.
- D. No officer shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- E. Officers shall verify an ALPR alert through the Ohio Law Enforcement Automated Data System (LEADS) before taking enforcement action that is based solely upon the ALPR alert.
- F. Access to LEADS data, when used in conjunction with ALPR data, is subject to all LEADS access regulations.
- G. All officers are required to log into the Flock System on their Mobile Data Terminal (MDT) at the start of their shift and log out of the system at the conclusion of their shift.

VI. ALPR DATA COLLECTION AND RETENTION

- A. All data and images gathered by an ALPR are for the official use of the Warren Police Department.
- B. LEADS data containing active NCIC records may be uploaded to the ALPR database on a regular basis. Because such data may contain confidential information, LEADS data is not open to public review.
- C. ALPR information gathered and retained by the Warren Police Department may be used and shared with prosecutors or other criminal justice agencies only as permitted by law and/or LEADS access regulations.
- D. ALPR data that becomes part of an investigation or criminal or civil action shall be downloaded to the Department's storage devices and retained in compliance with the Department's Record Retention

Schedule.

- E. Custom Hot List alerts can only be entered into the ALPR system with authorization from a supervisor or authorized detective.

VII. FLOCK STORAGE AND RETENTION

- A. FLOCK Group, Inc., the ALPR vendor, will store the ALPR data for no longer than 30 days and ensure proper maintenance and security of data stored in their cloud-based system. FLOCK will also oversee purging data at the end of the 30-day storage period. The Department is responsible for extracting, downloading, and archiving footage from FLOCK on its own storage devices for auditing, prosecutorial, and administrative purposes.
- B. All ALPR data is encrypted in transit from camera to cloud-based storage and encrypted at rest in the cloud-based storage.
- C. Information gathered or collected, and records retained by the FLOCK Safety System on the behalf of the Department, will not be:
 - 1. Sold, published, exchanged, or disclosed for commercial purposes.
 - 2. Disclosed or published without authorization.
 - 3. Disseminated to persons not authorized to access or use the information.

VIII. ACCOUNTIBILITY AND SAFEGUARDS

All saved data will be closely safeguarded and protected by both procedural and technological means. The Warren Police Department will observe the following safeguards regarding access to and use of stored data.

- A. All non-law enforcement requests for access to ALPR data shall be referred to the Criminal Investigations Division (CID) Commander and processed with applicable law and LEADS access regulations.
- B. All ALPR data shall be accessible only through a login/password-protected system capable of documenting all access to information by name, date, and time.
- C. Officers approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only. The corresponding incident number or case number shall be entered into the ALPR system when conducting a search of the data.

- D. ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes.
- E. The CID Commander shall conduct quarterly ALPR system access audits.
- F. The CID Commander shall purge expired local alerts at least every 60 days.

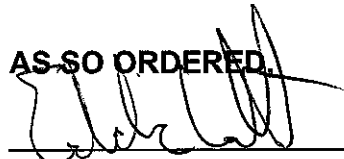
IX. CID ADMINISTRATIVE RESPONSIBILITIES

- A. Conduct quarterly ALPR system access audits.
- B. Purge expired local alerts at least every 60 days.
- C. Add, edit, or remove users.
- D. Request/revoke or approve/deny network access.
- E. Assign user roles.

END OF POLICY 24 – 001

The aforementioned rules, regulations, policy, procedure, to wit; PO/PR 24-001, be and the same, are ratified, prescribed, adopted, approved, made and promulgated, by me, on this 15th day, of MAY, 2024, at 1300 AM/PM

AS SO ORDERED



Eddie L. Colbert
Director of Public Service and Safety

The aforementioned rules, regulations, policy, procedure, to wit; PO/PR 24-001, be and the same, are ratified, prescribed, adopted, approved, made and promulgated, by me, on this 15 day, of MAY, 2024, at 1300 AM/PM

AS SO ORDERED



Eric J. Merkel
Chief of Police