Public Safety Video Surveillance System

338.1 PURPOSE AND SCOPE

This policy provides guidance for the placement and monitoring of CCSO public safety video surveillance, as well as the storage and release of the captured images.

This policy only applies to overt, marked public safety video surveillance systems operated by the CCSO. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the CCSO.

338.2 POLICY

The Calhoun County Sheriff's Office operates a public safety video surveillance system to complement its anti-crime strategy, to effectively allocate and deploy personnel, and to enhance public safety and security in public areas. Cameras may be placed in strategic locations throughout the County to detect and deter crime, to help safeguard against potential threats to the public, to help manage emergency response situations during natural and man-made disasters and to assist County officials in providing services to the community.

Video surveillance in public areas will be conducted in a legal and ethical manner while recognizing and protecting constitutional standards of privacy.

338.3 OPERATIONAL GUIDELINES

Only CCSO-approved video surveillance equipment shall be utilized. Members authorized to monitor video surveillance equipment should only monitor public areas and public activities where no reasonable expectation of privacy exists. The Sheriff or the authorized designee shall approve all proposed locations for the use of video surveillance technology and should consult with and be guided by legal counsel as necessary in making such determinations.

338.3.1 PLACEMENT AND MONITORING

Camera placement will be guided by the underlying purpose or strategy associated with the overall video surveillance plan. As appropriate, the Sheriff should confer with other affected County divisions and designated community groups when evaluating camera placement. Environmental factors, including lighting, location of buildings, presence of vegetation or other obstructions, should also be evaluated when determining placement.

Cameras shall only record video images and not sound. Recorded images may be used for a variety of purposes, including criminal investigations and monitoring of activity around high-value or high-threat areas. The public safety video surveillance system may be useful for the following purposes:

(a) To prevent, deter and identify criminal activity.

(b) To target identified areas of gang and narcotics complaints or activity.

(c) To respond to critical incidents.

Copyright Lexipol, LLC 2025/06/01, All Rights Reserved.
Published with permission by Calhoun County Sheriff's Office

(d) To assist in identifying, apprehending and prosecuting offenders.

(e) To document deputy and offender conduct during interactions to safeguard the rights of the public and deputies.

(f) To augment resources in a cost-effective manner.

(g) To monitor pedestrian and vehicle traffic activity.

Images from each camera should be recorded in a manner consistent with the underlying purpose of the particular camera. Images should be transmitted to monitors installed in the Shift Supervisor's office and Calhoun County Consolidated Dispatch Authority. When activity warranting further investigation is reported or detected at any camera location, the available information should be provided to responding deputies in a timely manner. The Shift Supervisor or trained Calhoun County Consolidated Dispatch Authority personnel are authorized to adjust the cameras to more effectively view a particular area for any legitimate public safety purpose.

The Sheriff may authorize video feeds from the public safety video surveillance system to be forwarded to a specified location for monitoring by other than sheriff's personnel, such as allied government agencies, road or traffic crews, or fire or emergency operations personnel.

Unauthorized recording, viewing, reproduction, dissemination or retention of anything documented by public safety surveillance equipment is prohibited.

338.3.2 CAMERA MARKINGS

All public areas monitored by public safety surveillance equipment shall be marked in a conspicuous manner with appropriate signs to inform the public that the area is under sheriff's surveillance. Signs should be well lit, placed appropriately and without obstruction to ensure visibility.

338.3.3 INTEGRATION WITH OTHER TECHNOLOGY

The CCSO may elect to integrate its public safety video surveillance system with other technology to enhance available information. Systems such as gunshot detection, incident mapping, crime analysis, license plate recognition, facial recognition and other video-based analytical systems may be considered based upon availability and the nature of CCSO strategy.

The CCSO should evaluate the availability and propriety of networking or otherwise collaborating with appropriate private sector entities and should evaluate whether the use of certain camera systems, such as pan-tilt-zoom systems, video enhancement or other analytical technology, requires additional safeguards.

338.4 VIDEO SUPERVISION

Supervisors should monitor video surveillance access and usage to ensure members follow CCSO policy and applicable laws. Supervisors should ensure such use and access is appropriately documented.

Copyright Lexipol, LLC 2025/06/01, All Rights Reserved.
Published with permission by Calhoun County Sheriff's Office

338.4.1 VIDEO LOG

A log should be maintained at all locations where video surveillance monitors are located. The log should be used to document all persons not assigned to the monitoring locations who have been given access to view or monitor images provided by the video surveillance cameras. The logs should, at a minimum, record the:

(a) Date and time access was given.

(b) Name and agency of the person being given access to the images.

(c) Name of person authorizing access.

(d) Identifiable portion of images viewed.

338.4.2 PROHIBITED ACTIVITY

Public safety video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

Public safety video surveillance equipment shall not be used in an unequal or discriminatory manner and shall not target individuals or groups based solely on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.

Video surveillance equipment shall not be used to harass, intimidate, or discriminate against any individual or group.

338.5 STORAGE AND RETENTION OF MEDIA

All downloaded media shall be stored in a secure area with access restricted to authorized persons. A recording needed as evidence shall be copied to a suitable medium and booked into evidence in accordance with established evidence procedures. All actions taken with respect to retention of media shall be appropriately documented.

The type of video surveillance technology employed and the manner in which recordings are used and stored will affect retention periods. The recordings should be stored and retained in accordance with the established records retention schedule.

338.5.1 EVIDENTIARY INTEGRITY

All downloaded and retained media shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

Copyright Lexipol, LLC 2025/06/01, All Rights Reserved.
Published with permission by Calhoun County Sheriff's Office

338.6 RELEASE OF VIDEO IMAGES

All recorded video images gathered by the public safety video surveillance equipment are for the official use of the Calhoun County Sheriff's Office.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for CCSO public records.

Requests for recorded images from other law enforcement agencies shall be referred to the Shift Supervisor for release in accordance with a specific and legitimate law enforcement purpose.

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established CCSO subpoena process.

338.7 VIDEO SURVEILLANCE AUDIT

The Sheriff or the authorized designee should conduct an annual review of the public safety video surveillance system. The review should include an analysis of the cost, benefit and effectiveness of the system, including any public safety issues that were effectively addressed or any significant prosecutions that resulted, and any systemic operational or administrative issues that were identified, including those related to training, discipline or policy.

The results of each review shall be appropriately documented and maintained by the Sheriff or the authorized designee and other applicable advisory bodies. Any recommendations for training or policy should be promptly addressed.

338.8 TRAINING

All CCSO members authorized to operate or access public safety video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, interaction with dispatch and patrol operations and a review regarding relevant policies and procedures, including this policy. Training should also address state and federal law related to the use of video surveillance equipment and privacy.

Copyright Lexipol, LLC 2025/06/01, All Rights Reserved.
Published with permission by Calhoun County Sheriff's Office

Automated License Plate Readers (ALPRs)

427.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

427.2 POLICY

The policy of the Eastpointe Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

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

427.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Eastpointe Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by theDeputy Chief or his designee. The Deputy Chief or his designee will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

427.4 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members 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 law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around 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.

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

Copyright Lexipol, LLC 2024/07/08, All Rights Reserved.
Published with permission by Eastpointe Police Department

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the appropriate official law enforcement database before taking enforcement action that is based solely on an ALPR alert.

427.5 DATA COLLECTION AND RETENTION

The Deputy Chief or his designee is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from cameras to the designated storage in accordance with department procedures.

All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.

427.6 ACCOUNTABILITY

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

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) ALPR system audits should be conducted on a regular basis.

427.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

Copyright Lexipol, LLC 2024/07/08, All Rights Reserved.
Published with permission by Eastpointe Police Department

(b) The request is reviewed by the Deputy Chief or the authorized designee and approved before the request is fulfilled.

(c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

Copyright Lexipol, LLC 2024/07/08, All Rights Reserved.
Published with permission by Eastpointe Police Department

Automated License Plate Readers (ALPRs)

427.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology. Our system used is the Flock Safety Camera (FSC) System.

Deter criminal behavior and assist in criminal investigations and prosecutions.

Enhance the department's efficiency and effectiveness, while enhancing community and officer safety with the use of FSC systems.

427.2 POLICY

The policy of the Hazel Park Police Department is to utilize FSC technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the FSC are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

427.3 ADMINISTRATION

The FSC technology, also known as Flock Safety Camera System (FSC), allows for the automated detection of license plates. It is used by the Hazel Park Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of FSC equipment, as well as FSC data retention and access, shall be managed by the Administration Lieutenant. The Administration Lieutenant will assign members under his/her command to administer the day-to-day operation of the FSC equipment and data.

427.4 OPERATIONS

Use of an FSC is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

(a) An FSC shall only be used for official law enforcement business.

(b) An FSC may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an FSC.

(c) While an FSC may be used to canvass license plates around any crime scene, particular consideration should be given to using FSC to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during

Copyright Lexipol, LLC 2025/01/13, All Rights Reserved.
Published with permission by Hazel Park Police Department

major crimes should be entered into the FSC system in an attempt to identify suspect vehicles.

(d) No member of this department shall operate FSC equipment or access FSC data without first completing department-approved training.

(e) No FSC operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the officer should verify an FSC response through the appropriate official law enforcement database before taking enforcement action that is based solely on an FSC alert.

(g) The following uses of the FSC system are prohibited : Use of the FSC system or associated scan file 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. Use of the FSC system or associated scan files or hot lists for any personal purpose.

427.5 ACCOUNTABILITY

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

(a) All FSC shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access FSC data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) FSC system audits should be conducted on a regular basis.

427.7 FSC DATA SHARING AND DISSEMINATION

The FSC data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a request for the FSC data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

(b) The request is reviewed by the Administration Lieutenant or the authorized designee and approved before the request is fulfilled.

(c) The approved request is retained on file.

Copyright Lexipol, LLC 2025/01/13, All Rights Reserved.
Published with permission by Hazel Park Police Department

(d) Unless the agency is a FSC reciprocating agency, only system administrators or supervisors will conduct searches of the FSC database for outside law enforcement agencies. The administrator or supervisor will enter the requesting agency's name, case number, and incident type in the reason for search field (i.e. OCSO 22-XXXXX Robbery).

FSC Data not deemed as evidence shall not be retained by this department.

The collection and storage of any FSC data shall only occur when it is deemed evidence in a criminal investigation. The collection and storage of evidence shall be done in accordance with the property room policy and records retention schedule.

427.7 DEFINITIONS

a. Alert - A visual and/or auditory notice that is triggered when the FSC system receives a potential "hit" on a license plate.

b. Fixed FSC system - FSC cameras that are permanently affixed to a structure, such as a pole traffic barrier, or a bridge.

c. Hit - A read matched to a plate within public view that has been registered on the agency's "hot lists" of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation, or which has been manually registered by a user for further investigation.

d. Hot Lists - License plate information of stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts that are regularly added to "hot lists" circulated among law enforcement agencies. Hot list information can come from a variety of sources including stolen vehicle information from the National Crime Information Center (NCIC), as well as national AMBER Alerts and Department of Homeland Security watch lists. Law enforcement agencies can interface their own locally compiled custom hot lists to the FSC system. These lists serve as an officer safety function as well as for investigative purposes. in addition to agency supported hot lists, designated users may also manually add license plate numbers to hot lists in order to be alerted if and when a vehicle license plate of interest is "read" by the FSC system.

e. FSC - Flock Safety Camera System.

f. Read - Digital images of license plates, vehicles, and associated metadata (e.g., date, time, and geographical coordinates associated with the vehicle image capture) that are captured by the FSC system.

427.8 FIXED FLOCK SAFETY CAMERA SYSTEMS (FSC) USAGE

a. Fixed FSC system is a passive system, live data is not viewed.

b. Fixed FSC systems monitors all license plates that come in the FSC camera's view.

Copyright Lexipol, LLC 2025/01/13, All Rights Reserved.
Published with permission by Hazel Park Police Department

c. The fixed FSC system provides the ability to search historical data. A log of such requests will be maintained by the system administrator.

d. All searches of the FSC system shall include a reason for the search, to include the case/ cfs number and type of incident (e.g., 22-xxxxx Robbery) Searches related to broadcasts by dispatch that do not have a case number, such as suspected drivers or vehicles wanted by other jurisdictions, will include "Broadcast" and the reason.

e. Fixed FSC Systems may have the ability to notify the system administrator and/or other police personnel of a " hit" from the LPR system "hot list".

427.9 FIELD OPERATIONS AND ENFORCEMENT ACTIONS

a. Custom hotlists that alert the entire organization or portions of the organization must be authorized by a detcetive, sergeant or command officer.

b. When notified of a NCIC "hit" from the FSC system, officers shall verify the the FSC response through the Law Enforcement Information Network (LEIN) before taking enforcement action. Action shall not be based solely on the FSC alert.

c. Occasionally, there may be errors in the FSC system's read of a license plate. Therefore, an alert alone is not a basis for police action.

d. Prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following:

1. Verification of a status on a hot list. An officer must confirm that the vehicle is stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances). Without confirmation, a vehicle cannot be stopped solely on a FSC alert and there must be a legal justification for the stop, such as a traffic violation, reasonable suspicion or probable cause.

2. Visual verification of license plate number. Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured(read) by the FSC, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding.

3. Because the FSC alert relates to a vehicle plate and may not relate to the person operating the vehicle, officers need reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle.

e. After the stop of a vehicle or other intervention based on the alert:

1. The officer will notify the supervisor of the positive hit and request that the plate be removed from the hot list, unless the interest in the vehicle still exists.

2. The officer will also notify the Detective Lieutenant of the removal via email or other reliable contact.

Copyright Lexipol, LLC 2025/01/13, All Rights Reserved.
Published with permission by Hazel Park Police Department

Automated License Plate Readers (ALPRs)

419.1 PURPOSE AND SCOPE

The purpose and scope of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

Attachment: Flock Training Acknowledgement

419.2 POLICY

Automated License Plate Reader (ALPR) technology provides automated detection and the capture of license plates through the use of fixed camera. ALPR will be used by the Jackson County Sheriff Office for official law enforcement purposes only, including identifying stolen or wanted vehicles, stolen license plates, missing persons and criminal investigation. The ALPR technology shall not be used for traffic violations, outstanding fines or any civil infractions. Further, it shall not be used to track or monitor individuals not currently involved in any other investigation.

All data and images gathered by the ALPR are for the official use of this office.

419.3 ADMINISTRATION

The Patrol Captain will oversee all ALPR operations and administrative oversight of the system. Additionally, the Patrol Captain will assign an appropriate designee (ALPR Administrator) to be responsible for managing the ALPR system. With Patrol Captain input, the ALPR Administrator will also be responsible for designing and implementing proper training, as well as maintaining training records for ALPR. The ALPR Administrator, will be responsible for ensuring the security and integrity of the data captured, stored and/or retained by the ALPR system, authorizing any requests for ALPR systems use or data access according to the policies and guidelines of the Sheriff Office and ensuring that all statutory reporting and public disclosure requirements regarding ALPR use are met.

419.3.1 USER ACCOUNTS

Only trained LEIN certified, law enforcement staff may access or search ALPR systems, data and associated media at the direction of the Sheriff or designee. The ALPR Administrator is responsible for creating user accounts for those officers who have successfully completed all appropriate training. The administrator is also responsible –with ensuring all authorized users complete the training requirements.Additionally, the ALPR Administrator is responsible for deleting or deactivating users once they separate from the department, fail to complete training or are otherwise no longer authorized to access ALPR data.

The ALPR Administrator will audit the list of all users at least once each quarter to ensure all of the users are still employed by the department and authorized to access ALPR data.

Copyright Lexipol, LLC 2024/05/09, All Rights Reserved.
Published with permission by Jackson County Office of the Sheriff

419.4 OPERATIONS

Use of ALPR is restricted to the purposes outlined below.

An ALPR shall only be used for official law enforcement business, and, if information is downloaded, it must be documented in a case report to include the basis for the inquiry, and the action taken.

(a) An ALPR may be used in conjunction with any patrol operation or criminal Investigation.

(b) ALPR may be used to canvass license plates around any crime scene, priority consideration should be given to major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

(c) The deputy shall verify an ALPR Hit Alert response through the appropriate official law enforcement database before taking enforcement action that is based solely on an ALPR Hit alert.

(d) Upon receiving a Hit Alert, the ALPRS Operator shall confirm that the observed license plate from the system matches the actual license plate of the observed vehicle.

419.5 DATA COLLECTION AND RETENTION

The Sheriff or designee, shall be responsible for ensuring systems and processes are in place for proper collection and retention of ALPR data.

All ALPR data downloaded to the third party server, not involving an infraction, should be stored for no longer than thirty (30) days. Therefore, it shall be purged, unless it has become, or it is reasonable to believe it will become evidence in a civil infraction, or a criminal action to produce records. In those circumstances, the applicable data should be downloaded from the server onto portable media and logged into evidence in accordance with department policy, and maintained with the case file.

The ALPR vendor will store the data (data hosting) and ensure proper maintenance and security of data stored in their data servers. The vendor will purge their data at the end of the 30 days of storage. This will not preclude the Jackson County Sheriff Office from maintaining any relevant vehicle data obtained from the system after that period as outlined elsewhere in this policy.

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

419.6 ACCOUNTABILITY AND SAFEGUARDS

All data will be closely safeguarded and protected by both procedural and technological means.

The Jackson County Sheriff's Office will observe the following safeguards regarding access to and use of stored data:

Copyright Lexipol, LLC 2024/05/09, All Rights Reserved.
Published with permission by Jackson County Office of the Sheriff

(a) All ALPR data downloaded to the computer or MDT and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation.

(c) A member searching through ALPR data must document the reason for the search, and the documentation shall be done in a manner which will allow for proper auditing (i.e. complaint number).

(d) All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law.

(e) Every ALPR Detection browsing inquiry must be documented by either the associated case number or incident number, and/or a reason for the inquiry.

419.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. For agencies without a mutual aid agreement, a letter of understanding, or other agreement in place,a written request from the requesting law enforcement agency shall include the name of the agency, the name of the person requesting, and the intended purpose for obtaining the information. Command approval is required. Approved requests for data shall be retained in accordance with record retention policies. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed in accordance with records release policies and the Freedom of Information Act (FOIA).

419.8 PROHIBITED USES

ALPR Operators may only access the use of the system for official and legitimate law enforcement purposes consistent with this policy. Also see policies 311, 314, 319,320. The following uses of the system are specifically prohibited:

(a) No member may use another member's account to access ALPR data.

(b) Invasion of Privacy: Except when done pursuant to court order such as a search warrant, it is a violation of this policy to utilize the APLR to record license plates except those of vehicles that are exposed to public view on roadways, generally open to the public.

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

(d) Use based on a protected class: It is a violation of this policy to use the ALPR system because of a person's, or group's, race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, age, or other classification protected by law.

(e) Personal Use: It is a violation of this policy to use the ALPR system for any personal use.

Copyright Lexipol, LLC 2024/05/09, All Rights Reserved.
Published with permission by Jackson County Office of the Sheriff

(f) First Amendment rights: It is a violation of this policy to use the ALPR system for the purpose or known effect of infringing upon a person's First Amendment rights.

(g) Designation of hot lists to be utilized by the ALPR system shall be made by the Sheriff or their designee. Hot lists shall be obtained or compiled from sources consistent with the purposes of the ALPR system set forth in this policy. An alert alone shall not be a basis for police action (other than following the vehicle of interest).

Anyone who engages in impermissible use of the ALPR system, or associated scan files, or hot lists may be subject to criminal prosecution, civil liability, and/or administrative sanctions pursuant to and consistent with collective bargaining agreement(s) and office and county policies. Discipline, up to and including discharge shall be considered in serious violations of this policy.

419.9 DATA DETECTION BROWSING AUDITS

A regular quarterly audit shall be conducted of ALPR detection browsing inquiries by the County Administrator's office. The audit shall be documented on a memorandum to the Board of Commissioners, and shall include any data errors found, so that they can be corrected. Additionally, the audit shall include the current permissible users.

Copyright Lexipol, LLC 2024/05/09, All Rights Reserved.
Published with permission by Jackson County Office of the Sheriff

Attachments

Copyright Lexipol, LLC 2024/05/09, All Rights Reserved.
Published with permission by Jackson County Office of the Sheriff

Flock Training Acknowledgement.pdf

Copyright Lexipol, LLC 2024/05/09, All Rights Reserved.
Published with permission by Jackson County Office of the Sheriff

JACKSON COUNTY
OFFICE OF THE SHERIFF
212 W. Wesley St. Jackson, Michigan 49201 Telephone: (517) 768-7900

Gary R. Schuette
Sheriff

Christopher A. Simpson
Undersheriff

Flock ALPR Training Acknowledgment

I, _____ acknowledge the following:
(Printed Name)

- I have received office-approved training on the use of Flock
- I have reviewed the office's policy on ALPR use
- I will abide by the office's training and policy

_____ _____
Signature / ID# Date

_____
Printed Name of Trainer

_____ _____
Signature / ID# of Trainer Date

Automated License Plate Readers (ALPRs)

427.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

427.2 POLICY

The policy of the Jackson Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

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

427.3 ADMINISTRATION

The ALPR technology allows for the automated detection of license plates. It is used by the Jackson Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

427.4 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members 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 law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR to canvass areas around 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.

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

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the appropriate official law enforcement database before taking enforcement action that is based solely on an ALPR alert.

Copyright Lexipol, LLC 2024/07/01, All Rights Reserved.
Published with permission by Jackson Police Department

427.5 DATA COLLECTION AND RETENTION

The Support Operations Division Commander is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data.

All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.

427.6 ACCOUNTABILITY

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

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) ALPR system audits should be conducted on a regular basis.

427.7 RELEASING ALPR DATA

ALPR data may be shared with other law enforcement or prosecutorial agencies upon request or through shared data on the vendor platform. The requesting agency must provide the reason for the request, and it can only be used for official law enforcement purposes.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

Copyright Lexipol, LLC 2024/07/01, All Rights Reserved.
Published with permission by Jackson Police Department

Automated License Plate Readers (ALPR)

428.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the Mount Vernon Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. The ALPR may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

428.2 ADMINISTRATION OF ALPR DATA

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administration Division Supervisor. The Administration Division Supervisor will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

428.3 ALPR OPERATION

Use of an ALPR is restricted to the purposes outlined below. Department personnel 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 business.

(b) An ALPR may be used in conjunction with any patrol operation or official Department investigation. Reasonable suspicion or probable cause is not necessary before using ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around 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.

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

(e) If practicable, the patrolman should verify an ALPR response through LEADS before taking enforcement action that is based solely upon an ALPR alert.

(f) No ALPR operator may access Ohio Law Enforcement Automated Data System (LEADS) data unless otherwise authorized to do so.

(g) ALPR notification access may be granted to outside agencies by the Chief of Police or designee.

(h) To adhere to reporting and retention requirements, ALPR search access will be governed as follows: Every conducted search and custom "Hotlist" must be linked to a Call-for Service (CFS) number or report number, which will include the reason for the search. Furthermore, ALPR searches by our department users for non-agency personnel will exclusively be conducted by designated agency personnel. All searches

Copyright Lexipol, LLC 2024/09/12, All Rights Reserved.
Published with permission by Mount Vernon Police Department

carried out by authorized personnel for non-agency individuals will include the case number and purpose for the requested action.

(i) For ongoing or active incidents, officers may enter "ai" for "Active Incident" in the "reason for search field" or the "case number" field when initiating a search or hotlist. The time of the ALPR search can be used at a later time if needed for cross reference with the corresponding CFS or case number based on the time of the event. To ensure officer safety and operational efficiency, this process will streamline the tracking of search requests while maintaining accountability. Officers will be able to quickly search current events, reducing delays in accessing critical information during high-pressure situations. Officers must still request that dispatch create a CFS and provide a reason for the CFS.

428.4 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Mount Vernon Police Department. Because such data may contain confidential information LEADS data is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law and this policy.

The Administration Division Supervisor is responsible to ensure proper collection and retention of ALPR data and for transferring ALPR data stored in department vehicles to the department server on a regular basis, not to exceed 30 days between transfers.

All ALPR data downloaded to the server should be stored for the minimum period established in the Department Records Retention Schedule identified in the Records Maintenance and Release Policy. Thereafter, ALPR data may be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

428.5 ACCOUNTABILITY AND SAFEGUARDS

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

(a) All non-law enforcement requests for access to stored ALPR data shall be referred to the Records Clerk and processed in accordance with applicable law.

(b) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

Copyright Lexipol, LLC 2024/09/12, All Rights Reserved.
Published with permission by Mount Vernon Police Department

(d) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes in accordance with this policy.

(e) ALPR system audits should be conducted on a regular basis.

Copyright Lexipol, LLC 2024/09/12, All Rights Reserved.
Published with permission by Mount Vernon Police Department

Automated License Plate Readers (ALPRs)

427.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

427.2 POLICY

The policy of the Napoleon Township Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

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

427.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Napoleon Township Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Chief of Police or Deputy Chief of Police. The Chief of Police or Deputy Chief of Police will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

427.4 RESPONSIBILITIES

It is the responsibility of any agent of the department that is authorized to utilize the approved ALPR systems to strictly adhere to the operations and safeguards within this policy. Failure to do so, or misuse of any ALPR device, system, or information is subject to disciplinary action, up to and including termination.

427.5 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members 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 law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass

Copyright Lexipol, LLC 2024/12/11, All Rights Reserved.
Published with permission by Napoleon Township Police Department

areas around 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.

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

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the appropriate official law enforcement database before taking enforcement action that is based solely on an ALPR alert.

427.6 DATA COLLECTION AND RETENTION

The Chief of Police or authorized designee is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.

427.7 ACCOUNTABILITY

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

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) ALPR system audits should be conducted on a quarterly basis as a minimum standard.

427.8 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a written request for the ALPR data that includes:

Copyright Lexipol, LLC 2024/12/11, All Rights Reserved.
Published with permission by Napoleon Township Police Department

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

(b) The request is reviewed by the Chief of Police or the authorized designee and approved before the request is fulfilled.

(c) The approved request is retained on file.

(d) Requests for remote access may be made by law enforcement agencies, that currently employ the same software, using the ALPR company's website. These requests shall be monitored and either approved or denied by the Chief of Police or authorized designee

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

Copyright Lexipol, LLC 2024/12/11, All Rights Reserved.
Published with permission by Napoleon Township Police Department

Flock Safety Camera System

435.1 PURPOSE AND SCOPE

Provide guidelines on the proper use of the Crime Prevention license plate recognition (LPR) system, also commonly known as the Flock Safety Camera (FSC) system.

Provide governmental accountability by ensuring the FSC system use respects the constitutional and privacy rights.

Deter criminal behavior, assist in criminal investigations and prosecutions, and aid in locating missing or endangered persons.

Allow for appropriate cooperation with businesses, institutions, condominium associations, homeowner associations, neighborhood associations, and other entities or groups seeking safety and security for specifically identified property.

Enhance the departments productivity and effectiveness, while enhancing community and officer safety with the use of the FSC systems.

435.2 DEFINITIONS

Alert – A visual and/or auditory notice that is triggered when the FSC system receives a potential "hit" on a license plate

Fixed FSC system – FSC cameras that are permanently affixed to a structure, such as a pole, traffic barrier, or a bridge.

Hit – A read matched to a plate within public view that has been registered on the agency's "hot lists" of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation, or which has been manually registered by a user for further investigation.

Hot Lists – License plate information of stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts that are regularly added to "hot lists" circulated among law enforcement agencies. Hot list information can come from a variety of sources, including stolen vehicle information from the National Insurance Crime Bureau and the National Crime Information Center (NCIC), as well as national AMBER Alerts and Department of Homeland Security watch lists. Departments of motor vehicles can provide lists of expired registration tags, and law enforcement agencies can interface their own locally compiled custom hot lists to the FSC system. These lists serve as an officer safety function as well as for investigative purposes. In addition to agency supported hot lists, designated users may also manually add license plate numbers to hot lists in order to be alerted if and when a vehicle license plate of interest is "read" by the FSC system.

FSC – Flock Safety Camera System

Read – Digital images of license plates, vehicles, and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the FSC system.

Copyright Lexipol, LLC 2024/08/20, All Rights Reserved.
Published with permission by Ottawa County Sheriff's Office

435.3 POLICY

The Ottawa County Sheriff's Office FSC system will not have an audio recording feature, nor shall modifications be made to the system to allow audio recording

435.3.1 AUTHORIZED USES AND USERS

- FSC systems, FSC data and associated media are the property of the Ottawa County Sheriff's Office and are to be used only in conducting the agency's official business.
- Only trained LEIN certified law enforcement staff or dispatchers may access or search FSC systems, FSC data, and associated media.
- The use of FSC systems associated equipment and databases are restricted to public safety-related missions of this agency and is authorized for law enforcement purposes only.
- Except when done pursuant to a court order such as a search warrant, the FSC may be used only to record license plates 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).

435.3.2 PROHIBITED USES

- Use of the FSC system or associated scan file 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.
- Use of the FSC system or associated scan files or hot lists for any personal purpose

435.4 ADMINISTRATION

The Sheriff (or designee) shall designate an employee(s) with administrative oversight (The Administrator) for FSC system deployment and operations who is responsible for the following;

- Establishing protocols for access. To ensure proper operation and facilitate oversight of the FSC 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.
- Establishing protocols for the entry, collection, storage, and retention of FSC data and associated media files.
- Authorizing any requests for FSC systems use of data access according to the policies and guidelines of this agency.

Designated personnel shall check equipment on a regular basis to ensure functionality and camera alignment.

- Any equipment that falls outside of expected functionality shall be reported immediately to Flock Safety.

FSC system repairs, hardware, or software, shall be made by technicians through Flock Safety.

Copyright Lexipol, LLC 2024/08/20, All Rights Reserved.
Published with permission by Ottawa County Sheriff's Office

435.5 FIXED FLOCK SAFETY CAMERA SYSTEMS (FSC) USAGE

Fixed FSC system is a passive system, live data is not viewed.

Fixed FSC systems monitors all license plates that come in the FSC camera's view.

The Fixed FSC system provides the ability to search historical data.

- A log of such requests will be maintained by the system administrator.

All searches of the FSC system shall include a reason for the search, to include the case /CAD number and type of incident (e.g., 22-XXXX Robbery).

- Searches related to broadcasts by dispatch that do not have a case/CAD number, such as suspected drivers or vehicles wanted by other jurisdictions, will include "Broadcast" and the reason (e.g., Broadcast – GRPD Shooting Suspect Vehicle).

Fixed FSC systems may have the ability to notify the system administrator and/or other police personnel of a "hit" from the LPR system "hot list."

435.6 FIELD OPERATIONS AND ENFORCEMENT ACTIONS

All users of the FSC system will un-select the following under the NCIC notification reasons, and will not take any enforcement action if the FSC system alerts solely for these reasons:

- Supervised Release
- Protection Order
- Violent Person
- Immigration Violator
- Sex Offender

Custom hotlists that alert the entire organization or portions of the organization must be authorized by a sergeant, or command officer.

The custom hotlist form must be completed to initiate entry into the FSC system.

- When there is a need for immediate entry by the OCCDA dispatch supervisor for serious crimes in progress or just occurred, the hotlist form must still be completed and forwarded to the Investigative Division.
- OCSO Flock Hot List Entry Form

The Investigative Division will be responsible for entry, removal, and auditing of the custom hotlist information.

When notified of a NCIC "hit" from the FSC system, officers shall verify the FSC response through the Law Enforcement Information Network (LEIN) before taking enforcement action.

- Action shall not be based solely on the FSC alert.

Copyright Lexipol, LLC 2024/08/20, All Rights Reserved.
Published with permission by Ottawa County Sheriff's Office

Occasionally, there may be errors in the FSC system's read of a license plate. Therefore, an alert alone is not a basis for police action.

Prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following;

- Verification of a status on a hot list.
    - An officer must confirm that the vehicle is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).Without confirmation, a vehicle cannot be stopped solely on a FSC alert and there must be a legal justification for the stop, such as a traffic violation, reasonable suspicion or probable cause.
- Visual verification of license plate number.
    - Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the FSC, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding.
- Because the FSC alert relates to a vehicle plate and may not relate to the person operating the vehicle, officers need reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle (for example, if a vehicle is entered into the system because of its association with a wanted individual, officers shall attempt to visually match the occupant to the description of the wanted subject associated to the vehicle plate or BOL prior to making a stop or should have another legal basis for making the stop).

After the stop of a vehicle or other intervention based on the alert:

- The officer will notify the patrol supervisor of the positive hit and request that the plate be removed from the hot list, unless the interest in the vehicle still exists.
- The officer will also notify the Investigative Division of the removal via department e-mail.

435.7 FCS DATA SHARING AND DISSEMINATION

FSC data should be considered for official use only and can only be shared for legitimate law enforcement purposes.

- Outside law enforcement agencies that are part of the FSC network may be allowed search access for legitimate law enforcement purposes.
    - Command approval for each agency is required.
- Trained Ottawa County Sheriff's Office personnel may conduct searches of the FSC database for outside law enforcement agencies.
    - Ottawa County Sheriff's Office Personnel will enter the requesting agency's name, the agency's case number, and incident type in the reason for search field (i.e. complaint number - Robbery).
    - Only matching returns will be shared with the agency.

Copyright Lexipol, LLC 2024/08/20, All Rights Reserved.
Published with permission by Ottawa County Sheriff's Office

- Outside law enforcement agencies requesting to receive alerts of hits from the FSC system must have a mutual aid agreement, letter of understanding, or other agreement in place with Ottawa County Sheriff's Office, and must have an Ottawa County Sheriff's Office approved policy related to the FSC system.
    - Command approval is required.
- All custom hot list data entries into the FSC system for hits and alerts for outside law enforcement agencies will be completed by Ottawa County Sheriff's Office designated administrators.

435.7.1 RETENTION OF FSC RELATED PHOTOS AND DATA

FSC related data is stored for a maximum of 30 days.

FSC data that is potential evidence must be transferred to and retained in the department's digital evidence storage system (DES).

435.7.2 BUSINESS AND HOME OWNER ASSOCIATION PARTNERSHIPS

Business Entities and Home Owner Associations

- May purchase and install FSC technology
- May provide inquiry/view access to the Ottawa County Sheriff's Office

Any publicly/privately owned Crime Prevention FSC Camera System that stores data on OCSO databases must be done according to the specifications, policies, and guidelines of this agency.

Any publicly/privately owned Crime Prevention FSC Camera System will not have access to search or view FSC data stored on the OCSO databases.

Copyright Lexipol, LLC 2024/08/20, All Rights Reserved.
Published with permission by Ottawa County Sheriff's Office

Attachments

Copyright Lexipol, LLC 2024/08/20, All Rights Reserved.
Published with permission by Ottawa County Sheriff's Office

OCSO Flock Hot List Entry Form.pdf

Copyright Lexipol, LLC 2024/08/20, All Rights Reserved.
Published with permission by Ottawa County Sheriff's Office

OTTAWA COUNTY SHERIFF'S OFFICE
FLOCK SAFETY CAMERA HOT LIST
ENTRY FORM

Enter onto Hot List

Enter as Saved Search

OCCDA entered – date: _____

FOR HOT LIST ENTRY:

Complaint Number:_____ Incident Type:_____

Reason to add to Hot List:

_____

_____

_____

Investigative Purposes ONLY (provide specifics above)

Probable Cause for Stop/Arrest or Warrant Information:

_____

_____

FOR SAVED SEARCH:

Vehicle Type:_____

License Plate Type: Regular Plate _____ or Temporary Plate _____

Vehicle Color:_____

Start Time:_____ End Time:_____

Name of Person Making the Request to Enter (Must be Sergeant/Command):

_____ Date:_____

FOR OFFICE STAFF:

Entered Date:_____ Removed Date:_____

Reason for Removal:_____

Automated License Plate Readers (ALPR)

437.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of Automated License Plate Reader (ALPR) technology by members of the Perrysburg Police Division. ALPRs are used by the Perrysburg Police Division to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. The ALPR may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

437.2 POLICY

Members of the Perrysburg Police Division shall only use ALPRs for official and legitimate law enforcement purposes, and in accordance with all applicable federal, state, and local laws and regulations as they pertain to the collection, use, and dissemination of data obtained through the ALPR system. The Chief of Police may revoke the ALPR system access of any member found to have acted in violation of any provision of this policy, or to have engaged in any other improper use of the system. Unauthorized use of the ALPR system, in violation of this policy or applicable law, may result in discipline, up to and including termination.

437.3 ADMINISTRATION OF ALPR DATA

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Deputy Chief of Police. The Deputy Chief of Police will assign personnel under their command to administer the day-to-day operation of the ALPR equipment and data.

The Designated Lieutenant is responsible for managing training, granting levels of access based on assignment, and maintaining records of significant incidents and arrests that are related to ALPR usage.

437.4 ALPR OPERATION

Use of an ALPR is restricted to the purposes outlined below. Division personnel 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 business.

(b) An ALPR may be used in conjunction with any patrol operation or official Division investigation. Reasonable suspicion or probable cause is not necessary before using ALPR.

(c) An ALPR may be used to canvass license plates around any crime scene or other major incidents. Partial license plates and suspect vehicle descriptions, reported during major crimes, may be entered into the ALPR system in an attempt to identify suspect vehicles.

(d) No member of this Division shall operate ALPR equipment or access ALPR data without first completing Division-approved training.

Copyright Lexipol, LLC 2024/06/20, All Rights Reserved.
Published with permission by Perrysburg Police Division

(e) The officer shall verify an ALPR response through the Ohio Law Enforcement Automated Data System (LEADS) before taking enforcement action that is based solely upon an ALPR alert.

(f) Upon receiving an ALPR alert, prior to the initiation of the stop, officers and/or dispatchers shall do the following:

1. Visually verify that the vehicle plate alerted by the ALPR system matches the physical plate on the vehicle (numbers, letter, and state).
2. Upon visual verification of the plate, the officer shall verify the information through LEADS.

(g) No ALPR operator may access LEADS data unless otherwise authorized to do so.

(h) Logging into the ALPR system is only authorized on city owned devices (computers, cell phones, tablets, etc.)

437.5 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Perrysburg Police Division. Because such data may contain confidential information from LEADS, the data is not open to public review. ALPR information gathered and retained by this Division may be used and shared with prosecutors, law enforcement, or others only as permitted by law.

All ALPR data will be maintained by a third party vendor, Flock Safety, for a period of thirty days. Thereafter, ALPR data may be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence. Any downloaded data will then be maintained in conjunction with the associated case file as directed by the Records Maintenance and Release policy.

437.6 ACCOUNTABILITY AND SAFEGUARDS

All ALPR data will be closely safeguarded and protected by both procedural and technological means. The Perrysburg Police Division will observe the following safeguards regarding access to and use of ALPR data:

(a) All non-law enforcement requests for access to ALPR data shall be referred to the Support Services Manager and processed in accordance with applicable law.

(b) 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.

(c) Members shall not share login information with others and shall only use their login credentials to log into the system.

(d) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or Division-related civil or administrative action.

Copyright Lexipol, LLC 2024/06/20, All Rights Reserved.
Published with permission by Perrysburg Police Division

1. When conducting a search of ALPR data, members are required to enter the corresponding case number in the reason field.
2. When information is obtained through the use of an ALPR results in official action being taken, it shall be documented in the incident report.

(e) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes.

(f) ALPR system audits shall be conducted by the Designated Lieutenant at least every 30 days.

Copyright Lexipol, LLC 2024/06/20, All Rights Reserved.
Published with permission by Perrysburg Police Division

Automated License Plate Readers (ALPR)

424.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the Perrysburg Township Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. The ALPR may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

424.2 ADMINISTRATION OF ALPR DATA

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administration Division Supervisor. The Administration Division Supervisor will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

424.3 ALPR OPERATION

Use of an ALPR is restricted to the purposes outlined below. Department personnel 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 business.

(b) An ALPR may be used in conjunction with any patrol operation or official Department investigation. Reasonable suspicion or probable cause is not necessary before using ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around 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.

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

(e) If practicable, the officer should verify an ALPR response through LEADS before taking enforcement action that is based solely upon an ALPR alert.

(f) No ALPR operator may access Ohio Law Enforcement Automated Data System (LEADS) data unless otherwise authorized to do so.

424.4 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Perrysburg Township Police Department. Because such data may contain confidential information LEADS data is not

Copyright Lexipol, LLC 2024/06/27, All Rights Reserved.
Published with permission by Perrysburg Township Police Department

open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

The Administration Division Supervisor is responsible to ensure proper collection and retention of ALPR data and for transferring ALPR data stored in department vehicles to the department server on a regular basis, not to exceed 30 days between transfers.

All ALPR data downloaded to the server should be stored for the minimum period established in the Department Records Retention Schedule identified in the Records Maintenance and Release Policy. Thereafter, ALPR data may be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

424.5 ACCOUNTABILITY AND SAFEGUARDS

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

(a) All non-law enforcement requests for access to stored ALPR data shall be referred to the Records Supervisor and processed in accordance with applicable law.

(b) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(d) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes.

(e) ALPR system audits should be conducted on a regular basis.

Copyright Lexipol, LLC 2024/06/27, All Rights Reserved.
Published with permission by Perrysburg Township Police Department

Automated License Plate Readers (ALPRs)

422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology, referred to as the Flock Safety Camera (FSC) System.

422.1.1 DEFINITIONS

(a) Alert – a visual and or auditory notice that is triggered when the FSC system receives a potential "hit" on a license plate or vehicle indicator.

(b) Fixed FSC system – FSC cameras that are permanently affixed to a structure.

(c) Hit – A read matched to a plate within public view that has been registered on the agency's hot list of vehicles plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation or which has been manually registered by a user for further investigation.

(d) Hot List – License plate information of stolen cars, stolen registration plates, vehicles owned by persons of interest, vehicles associated with AMBER Alerts and vehicles associated with missing persons that are regularly added to hot lists circulated among law enforcement agencies. Hot list information can come from a variety of sources, including stolen vehicle information from the national Insurance Crime Bureau and the National Crime Information Center (NCIC) as well as the national AMBER Alerts and Department of Homeland Security watch lists. These lists serve as an officer safety function as well as for investigative purposes.

(e) FSC – Flock Safety Camera System

(f) Read – Digital images of license plates, vehicles, and associated metadata that are captured by the FSC system.

422.2 POLICY

The policy of the City of St. Joseph Department of Public Safety is to utilize ALPR technology to capture and store digital license plate data and images to deter criminal behavior and assist in criminal investigations and prosecutions, while recognizing the established privacy rights of the public.

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

422.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the City of St. Joseph Department of Public Safety to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be

Copyright Lexipol, LLC 2024/08/09, All Rights Reserved.
Published with permission by City of St. Joseph Department of Public Safety

used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administration Deputy Director. The Administration Deputy Director will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

422.4 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members 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 law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around 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.

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

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the public safety officer should verify an ALPR response through the appropriate official law enforcement database before taking enforcement action that is based solely on an ALPR alert.

422.5 DATA COLLECTION AND RETENTION

The Administration Deputy Director is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.

Copyright Lexipol, LLC 2024/08/09, All Rights Reserved.
Published with permission by City of St. Joseph Department of Public Safety

422.6 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The City of St. Joseph Department of Public Safety will observe the following safeguards regarding access to and use of stored data:

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) ALPR system audits should be conducted on a regular basis.

422.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

(b) The request is reviewed by the Administration Deputy Director or the authorized designee and approved before the request is fulfilled.

(c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

Copyright Lexipol, LLC 2024/08/09, All Rights Reserved.
Published with permission by City of St. Joseph Department of Public Safety

Automated License Plate Readers (ALPR)

428.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the Sylvania Township Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. The ALPR may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

428.2 ADMINISTRATION OF ALPR DATA

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Deputy Chief. The Deputy Chief will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

The Operations Lieutenant or their designee will assign user permissions to authorized agency personnel, and will also be responsible for granting camera access to other law enforcement agencies requesting access. As a general rule, the Sylvania Township Police Department will grant camera access to any requesting agency in Ohio, any other state, and any requesting Federal agency.

428.3 ALPR OPERATION

On-duty patrol officers are required to log in to the ALPR data system at the beginning of their shift and monitor for hot list alerts while on patrol.

Use of an ALPR is restricted to the purposes outlined below. Department personnel 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 business.

(b) An ALPR may be used in conjunction with any patrol operation or official Department investigation. Reasonable suspicion or probable cause is not necessary before using ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around 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.

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

(e) If practicable, the officer should verify an ALPR response through LEADS before taking enforcement action that is based solely upon an ALPR alert.

(f) No ALPR operator may access Ohio Law Enforcement Automated Data System (LEADS) data unless otherwise authorized to do so.

Copyright Lexipol, LLC 2024/06/17, All Rights Reserved.
Published with permission by Sylvania Township Police Department

(g) Each time the 'Search' or 'Look Up' tools are used in the ALPR, the member shall input either a CAD call number, report, or case number into the 'Search Reason' box.

The following uses of the ALPR hardware or software, are strictly prohibited:

A. **Invasion of Privacy:** Except when done pursuant to a court order or 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. Vehicles exposed to public view include vehicles on a public road or street, or that are on private property which is visible from a public road, street or a place where the general public has access, such as parking lots of publicly accessible businesses.

B. **Harassment or Intimidation:** It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

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

D. **Personal Use:** It is a violation of this policy to use the ALPR system, associated files, or hot lists for any personal purpose.

428.4 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Sylvania Township Police Department. Because such data may contain confidential information LEADS data is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

The ALPR vendor, will store the data (data hosting) and ensure proper maintenance and security of data stored on their servers. The ALPR vendor will purge collected data after 30 days of storage, however, this will not preclude members of the Sylvania Township Police Depratment from maintaining any relevant vehicle data obtained from the ALPR vendor after the period of 30 days.

All ALPR data downloaded to the server should be stored for the minimum period established in the Department Records Retention Schedule identified in the Records Maintenance and Release Policy. Thereafter, ALPR data may be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

428.5 ACCOUNTABILITY AND SAFEGUARDS

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

Copyright Lexipol, LLC 2024/06/17, All Rights Reserved.
Published with permission by Sylvania Township Police Department

(a) All non-law enforcement requests for access to stored ALPR data shall be referred to the Records Clerk and processed in accordance with applicable law.

(b) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(d) Such 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 Operations Lieutenant or designee shall conduct and document an annual audit of the ALPR access log to ensure compliance to this policy.

Copyright Lexipol, LLC 2024/06/17, All Rights Reserved.
Published with permission by Sylvania Township Police Department

Automated License Plate Readers (ALPRs)

426.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

426.3 POLICY

The policy of the Utica Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

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

426.4 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Utica Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by theChief of Police. The Chief of Police will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

426.5 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members 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 law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around 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.

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

Copyright Lexipol, LLC 2025/01/30, All Rights Reserved.
Published with permission by Utica Police Department

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the appropriate official law enforcement database before taking enforcement action that is based solely on an ALPR alert.

426.6 DATA COLLECTION AND RETENTION

The Chief of Police is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.

426.7 ACCOUNTABILITY

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

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) ALPR system audits should be conducted on a regular basis.

426.8 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

Copyright Lexipol, LLC 2025/01/30, All Rights Reserved.
Published with permission by Utica Police Department

(b) The request is reviewed by theChief of Police or the authorized designee and approved before the request is fulfilled.

(c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

Copyright Lexipol, LLC 2025/01/30, All Rights Reserved.
Published with permission by Utica Police Department