

Columbus Police Division Directive	EFFECTIVE Sep. 30, 2026	NUMBER 11.08
	REVISED	TOTAL PAGES 10
Sensor Technologies		



Cross Reference: 10.01, TS 11-11

I. Introduction

Law enforcement is an ever-changing and evolving profession. Technological advancements provide law enforcement personnel access to tools that can improve productivity and case solvability. One such advancement is the use of sensor technologies. The goal of the Division is to use these tools to enhance public safety, officer productivity, and investigative capability while safeguarding civil liberties and personal privacy and maintaining data integrity. This directive provides guidelines for data retention, access and use of sensor technology, and system audits to ensure compliance.

II. Definitions

A. Automated License Plate Reader (ALPR)

An electronic sensor that detects and analyzes license plates and vehicle descriptors. ALPRs may be mounted in a fixed location, on vehicles or trailers, or integrated into other devices, for example, the Cruiser Video System (CVS).

B. Automated License Plate Data Read

Information detected and recorded by an ALPR, which includes license plate numbers, vehicle photographs, time stamps, and location details.

C. Community Camera Registry

A list of privately-owned cameras (personal or business) where the owner has voluntarily provided his or her contact information and the location of the camera to aid law enforcement personnel in locating video footage to further criminal investigations.

D. Gunshot Detection System

Acoustic surveillance technology that uses sensors to detect, locate, and alert law enforcement agencies of potential gunfire incidents.

E. Hotlist

A list of identified license plate numbers within an ALPR system that are of law enforcement interest. Hotlists are utilized by local law enforcement, are separate from state and national databases, and are not shared across different ALPR systems. Adding a license plate to a hotlist will alert a user when a Division ALPR detects the license plate and may alert if the license plate is detected on an ALPR owned by another entity.

F. Mobile Trailer Camera

A camera system mounted on a portable trailer that contains its own power source and network connectivity. A mobile trailer camera typically has lenses pointed in different directions to produce multiple video feeds, and is used to increase monitoring capabilities for planned events or in areas where there has been an increase in crime.

G. Neighborhood Safety Cameras

A network of video cameras owned by the Department of Public Safety that are deployed based on calls for service statistics and safety initiatives for the purpose of enhancing public safety and improving crime solvability. The PoliceNET Unit coordinates the installation and maintenance of the cameras.

H. Real-Time Crime Center (RTCC) Software Solution

Software that integrates sensor technologies and computer-aided dispatch (CAD) data into a single platform that is typically map-based. RTCC software solutions allow personnel to more efficiently search various sensor technology systems and databases.

I. Sensor Technology System

Electronic devices and equipment used to passively observe, detect, analyze, or record individuals, vehicles, locations, or specific occurrences and the software used to access the data. Examples of sensor technology include ALPRs, camera feeds, and gunshot detection systems. This does not include systems that require manual control, piloting, or initiation, such as video feeds from a drone or helicopter.

J. Sensor Technology Impact Report

A report used in making sensor technology purchasing and deployment decisions that contains the following:

1. A description of the sensor technology, including how it works.
2. The purpose of the new sensor technology.
3. How the sensor technology will be deployed. If not uniformly throughout the City, include what criteria will be used to determine deployment location(s).
4. The fiscal impact, including both initial and ongoing costs.
5. Any anticipated civil rights or civil liberty concerns the community may have about the new sensor technology and a plan to address those concerns.

K. Third-Party Camera Feeds

Public-facing video feeds that the Division has been granted access to from cameras owned and maintained by a private entity. Terms of the access are set by the owner and detailed in an agreement between the owner or authorized representative and the Department of Public Safety.

L. Virtual Patrol

The use of sensor technology to check an area for illegal activity or evidence of a crime from a remote location.

III. Policy Statements

A. Access

1. Sensor technology software and data access shall be limited to sworn personnel, crime analysts, criminal intelligence analysts, and other civilian personnel when access is permitted by their bureau SOP.
2. Sensor technology equipment shall only be accessed by Technical Services Section (TSS) personnel.
3. Division personnel shall only access sensor technology systems from a Division-owned device. Personnel shall not use a personally owned or non-encrypted device to access sensor technologies.
4. Division personnel shall not access any sensor technology system when off-duty.
5. Division personnel shall only use approved websites or applications to access sensor technologies.
6. Division personnel shall not utilize any sensor technology systems until they receive training that includes specific instructions for the specific sensor technology and any applicable policies.
7. Division personnel granted access to sensor technology systems shall receive initial training and subsequent annual refresher training on this directive and the "Division Computer Systems and Mobile Devices" directive.
8. The PoliceNET Unit shall be responsible for sensor technology system access control. This includes onboarding; user management; and suspension, revocation, and reinstatement of access.

B. Use of Sensor Technology Systems

1. Division personnel shall only access sensor technology systems for official law enforcement purposes.
2. Division personnel shall not access sensor technology systems or utilize sensor technology data for any of the following:
 - a. Personal gain or any situation in which they have a personal interest
 - b. To gather information solely based on First Amendment protected activity
 - c. For the purpose of detecting or apprehending persons based on suspected immigration status, unless a judicial warrant exists, a criminal violation was reported, or an arrest was made
 - d. To restrict access to or gather information regarding reproductive care
 - e. To harass or intimidate any individual or group

- f. To target any individual based solely on the person's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other class protected by law
 - g. For any reason that would violate an individual's Constitutional Rights, Division policy, or the law
3. Sensor technology utilized by Division personnel shall only monitor areas where individuals do not have an expectation of privacy, unless exigent circumstances exist or a warrant has been obtained.

Note: The PoliceNET Unit is responsible for adding privacy blocks in the Neighborhood Safety Camera system to prevent viewing inside private residences.

- 4. Division personnel shall only use sensor technology object detection or artificial intelligence capabilities when they have a reason to believe the person or object being searched for is involved in criminal activity or there is a public safety concern.
- 5. Sensor technologies are considered law enforcement databases and are subject to the same safeguards and restrictions. Misuse of sensor technology, data, equipment, software, applications, or log-in credentials may be considered critical misconduct and could violate local, state, or federal law. Refer to the "Division Computer Systems and Mobile Devices" directive.
- 6. Division supervisors shall review the weekly report of all ALPR searches conducted by their subordinates and document the review as directed in the notification email. Division supervisors shall immediately notify the chain of command through the commander if any violations of policy are suspected.

C. Sensor Technology Data

- 1. Sensor technology data shall be treated as Criminal Justice Information for the purposes of data protection and personnel shall ensure it is safeguarded from unauthorized access or use.
- 2. Regardless of sensor ownership or deployment reason, Division personnel shall only access sensor technology data and the associated software for law enforcement purposes.
- 3. Division personnel shall not share, sell, transmit, or disseminate sensor technology data to any non-law enforcement entity except as required by law or when approved by the Chief of Police or designee.
 - a. All requests from non-law enforcement entities shall be referred to the Public Records Bureau.
 - b. The Chief of Police or designee shall determine when the Division will grant other law enforcement agencies direct access to sensor technology data through the software application and when the Division will request such access from another agency.
 - c. The Division will immediately suspend an agency's direct access when made aware of any potential misuse or security threat.

4. Sensor technology data shall be retained in accordance with the following table unless identified as evidence in an investigation:

Sensor Technology	Retention Period	Data Ownership	Storage Location
Neighborhood Safety Cameras	14 Days	City of Columbus Department of Public Safety	Department of Technology Servers
Other City of Columbus Cameras	Varies by Facility	Department of Technology	Department of Technology Servers
ALPRs	7 Days	Division of Police	Cloud-Hosted
ShotSpotter® Gunshot Detection	Indefinite	Division of Police	Cloud-Hosted
Third-Party Camera Feeds	Varies by Owner	Third-Party	Varies by System

5. Sensor technology data with evidentiary value shall be uploaded to the Division's evidence management system or saved in accordance with the applicable SOP. If another officer is investigating the incident, personnel should communicate with him or her regarding any evidence uploaded to the case file.

Note: Using a bookmark in the sensor technology software does not retain the data beyond the standard retention period.

6. Division personnel shall only download sensor technology data on a Division computer or Division-issued electronic device. Division personnel shall not download, save, or digitally capture sensor technology data on any personally owned device.
7. Division personnel shall not duplicate or download sensor technology data/photos/videos unless necessary for a legitimate administrative or law enforcement purpose (for example, to further a case or investigation or to send a copy to the prosecutor).
8. Division personnel shall destroy any printouts of sensor technology data when they are no longer needed.

D. ALPR Alerts

1. Sworn personnel receiving an ALPR alert, commonly referred to as a "hit," shall verify that the vehicle matches the vehicle in the alert.
2. Sworn personnel shall not stop or detain an individual(s) solely on the basis of an ALPR alert.
- a. Sworn personnel shall evaluate the nature of the alert and determine if there is a lawful reason for the stop.

- b. When applicable, sworn personnel shall utilize other law enforcement databases to verify the validity of an alert (for example, verifying a wanted person or stolen vehicle alert in LEADS).
 - 3. Sworn personnel shall include information pertaining to the alert in the narrative section of the Arrest Information, form U-10.100, whenever an arrest or summons is completed.
 - 4. Sworn personnel shall also check the "LPR Used to Apprehend/Identify" box on the Offenders Tab while completing a case report in the electronic reporting system when an ALPR is used to apprehend or identify an arrestee.
- E. Division personnel performing a search in a sensor technology software shall accurately complete all mandatory fields. Mandatory fields are marked with an asterisk.
- F. Hotlists
- 1. No license plate shall be added to a hotlist unless there is reasonable suspicion that the vehicle is associated with a criminal offense or an exigent circumstance involving public safety.
 - 2. A vehicle sought out of a case assigned to an investigative unit shall not be added to a hotlist unless directed by the primary investigator.
 - 3. Division personnel shall request supervisor approval to add a license plate to a hotlist.
 - 4. Division personnel who add or request the addition of a license plate to a hotlist shall ensure it is removed once the vehicle is no longer sought for a law enforcement purpose.
- G. Administration
- 1. Sensor Technology Deployment
 - a. The TSS Lieutenant shall be responsible for the deployment of sensor technology equipment and for managing sensor technology contracts, to include funding requests when applicable. Division personnel may be required to provide justification for the continuing funding of sensor technology solutions.
 - b. Division personnel requesting the purchase or deployment of new sensor technology equipment or systems shall submit a written proposal that includes a sensor technology impact report through the chain of command to the Support Subdivision Deputy Chief.
 - c. Common factors considered when determining deployment locations include, but are not limited to, the following:
 - (1) Public safety concerns
 - (2) Rights of individuals within the monitored area
 - (3) Areas known to have criminal activity
 - (4) Requests from the community
 - (5) Requests from Division personnel

- (6) Requests from other law enforcement agencies
- (7) Availability of a suitable source of power and data connectivity
- (8) Safety of installation personnel
- (9) Purpose of the deployment
- (10) Potential impact on the community
- (11) Funding availability

2. Audits

- a. All sensor systems utilized by the Division shall document the date, time, user, and reason for all queries.
- b. The TSS Lieutenant shall conduct audits of ALPR usage every other month and an annual review of the audit findings.
- c. The TSS Lieutenant shall conduct an annual review of sensor technology policies and recommend revisions as needed.
- d. Personnel requesting an audit of an employee's sensor technology usage shall follow the policies and procedures outlined in the "Division Computer Systems and Mobile Devices" directive.

3. The PoliceNET Unit shall be responsible for the following:

- a. Deployment logistics and maintenance of sensor technology equipment and software
- b. Access control
- c. Technical support

H. Personnel shall not attempt to repair any sensor technology equipment or software. Contact the PoliceNET Unit or submit a TechDesk ticket to request support.

IV. Procedures

A. Access Management

1. Requesting Personnel

- a. Request access by submitting a ticket through the "TechDesk" application located on the desktop.
- b. Contact the TSS Lieutenant and request to be enrolled in the initial training.
- c. Complete all assigned training and document reviews in the document management system to maintain certification.
- d. To request reinstatement after access is terminated, send a letter through the chain of command to your deputy chief.

2. TSS Lieutenant

- a. Coordinate training for all Division employees approved to utilize sensor technologies.
- b. Maintain a record of all certified users for each sensor technology.

- c. Direct PoliceNET Unit personnel to revoke access for any user that does not complete any training or document acknowledgement required to maintain certification.
 - d. Coordinate reinstatement when approved by a deputy chief and maintain a record of all denied requests.
3. PoliceNET Unit Personnel
- a. Review requests for sensor technology access. If the individual is not in a job classification or assignment that automatically qualifies for access, forward the request to the requestor's commander for approval.
 - b. Process access requests for authorized personnel.
 - c. Maintain a record of any access requests that are denied.
 - d. When directed by the TSS Lieutenant, terminate system access.
4. Commander
- Approve or deny access requests received from the PoliceNET Unit personnel and advise them of the decision in writing.
5. Deputy Chief
- Make the final decision on requests for reinstatement and forward the letter to the TSS Lieutenant.
- B. Adding a Plate to a Hotlist
- 1. Upon supervisor approval, create a hotlist entry in the ALPR system.
 - 2. Enter the license plate information (plate number and state).
 - 3. In the "Case Number" field, enter the incident number.
 - 4. Set the expiration date. The expiration date should be set as 14 days unless justification exists to extend the duration.
 - 5. In the "Reason" field, enter the following information:
 - a. The justification for adding the plate to the hotlist (for example, "Vehicle used in robbery").
 - b. The name(s) and description(s) of any suspects associated with the vehicle and whether or not any charges have been filed.
 - 6. In the "Notes" field, enter the vehicle description, the name and badge number of the approving supervisor, and any other pertinent information.
- C. Requesting a Mobile Trailer Camera
- 1. Requestor
 - a. Submit a request through your chain of command to the commander that includes the following information:
 - (1) Reason for the request
 - (2) Dates and times the camera(s) are needed
 - (3) Location

2. Commander
 - a. Recommend approval or deny the request.
 - b. If recommending approval, forward the request to the TSS Lieutenant.
3. TSS Lieutenant
 - a. Review requests and make a recommendation based on operational need and equipment availability.
 - b. Coordinate approval through the Special Events Section chain of command.
 - c. Advise the requestor of the approval decision.
 - d. Coordinate deployment for approved requests.
- D. Requests to Acquire or Utilize New Sensor Technology Systems
 1. Requesting Personnel
 - a. Send a letter through the chain of command to your assistant chief.
 - b. Include a Sensor Technology Impact Report.
 2. Deputy Chief
 - a. Recommend approval or deny the request.
 - b. If recommending approval, forward the request to the Support Services Subdivision Deputy Chief.
 3. Support Services Subdivision Deputy Chief
 - a. Document any concerns (for example, fiscal or technological issues), make a recommendation, and forward to the appropriate assistant chief.
 - b. When notified of an approved request, coordinate with the appropriate stakeholders to ensure a successful deployment.
 4. Assistant Chief
 - a. Recommend approval or deny the request.
 - b. If recommending approval, forward the request to the Chief of Police.
 5. Chief of Police
 - a. Recommend approval or deny the request.
 - b. If recommending approval, forward the request to the Director of Public Safety.
- E. TSS Lieutenant
 1. ALPR Audits
 - a. Review system audit and event logs to look for anomalies.
 - b. Review information from other sources (for example, the CAD, electronic reporting system, and case files) to determine the nature of the anomaly.
 - c. If further investigation is required, notify the commander of the involved personnel.
 - d. Document the disposition of any cases referred for investigation.

2. Annual Review

- a. Conduct an annual review of all sensor technology policies and procedures and recommend any changes necessary to ensure the Division is following current best practices.
- b. By March 31 of each year, submit an “Annual Sensor Technology Report” to the Chief of Police that includes the previous year’s audit results as well as any policy recommendations.
- c. After the report is approved by the Chief of Police, send it to the Division’s Webmaster to be posted on the Division’s public-facing website.