NASHVILLE DEPARTMENT OF TRANSPORTATION & MULTIMODAL INFRASTRUCTURE

INSTRUCTIONAL AND INFORMATIONAL MEMORANDUM

SECTION: 204 Information Technology	**POLICY NUMBER:** 204.011.2024
SUBJECT: Surveillance Usage and Privacy Policy for NDOT	**SUPERSEDES:**
APPROVED BY: Diana W. Alarcon	**APPROVED DATE: 9/6/2024**
APPLICABLE CODES/ORDINANCES: 13.08.080	

EFFECTIVE DATE: 9/6/2024

PURPOSE:

The purpose of this policy is to develop a surveillance use and privacy policy that is applicable throughout the department and consistent with Metro Code in data retention, access, and protection.

Policy:

Definitions

"Surveillance technology" shall mean any electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software. **"Surveillance technology" does not include technology or equipment that collects data in anonymized form or that immediately deletes or destroys non-anonymized collected data.**

"Personally identifiable information" or "PII" shall mean any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which any governmental department or agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, and other descriptors). Additionally, information

permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This definition includes information that is maintained in either paper, electronic or other media. **"Allowed PII" shall mean the image of a license plate, the time and location stamp of an image of a license plate, and the make, model, and color of the vehicle associated with an image of a license plate.**

Authorized and Prohibited Uses

Surveillance technology shall only be used to monitor a location within the county for official NDOT business. The technology shall be positioned in a lawful public location; or on private property with the consent of the owner or custodian of the property; or pursuant to a valid court order.

Authorized purposes for using surveillance technology include traffic management, parking enforcement, illegal dumping, fleet management, curb management, and asset management. The following definitions will be used for this policy:

Traffic management – Planning, monitoring, control, and optimization of traffic flow to ensure the safe and efficient movement of vehicles and pedestrians for non-law enforcement purposes.

Parking enforcement – Enforcing parking code, Traffic and Parking Commission regulations and NDOT policies in the Metropolitan government area.

Illegal dumping – Enforcing the provisions of the Metropolitan Code concerning the unauthorized disposal of waste in areas not designated for waste collection in the Metropolitan government area.

Fleet management – The deployment of an Automatic Vehicle Location (AVL) system to determine and transmit the geographic location of a NDOT vehicle to track and manage vehicle movements in real-time.

Curb management – Enforcing the provisions of the Metropolitan Code, Traffic and Parking Commission regulations and NDOT policy concerning the curb such as parking, loading, public transportation, and pedestrian access.

Asset management – The strategic and systematic process of operating, maintaining, upgrading, and expanding physical transportation assets throughout their lifecycle.

Authorized personnel include NDOT engineers, technicians, supervisors, and IT professionals. Personnel authorized to use NDOT's systems shall be specifically trained in the system and the NDOT usage and privacy policy prior to receiving account access. Authorized user accounts which are inactive for a period of six months will be disabled automatically. Authorized users with disabled accounts must be retrained in accordance with 13.08.080. Users found to have used the system without authorization, with improper credentials, or in a manner not authorized shall have their access immediately revoked and may face disciplinary action.

Data Collection

Surveillance technology shall be activated by movement and record video and photo images. The Transportation Management Center (TMC) may use technology/equipment for the sole and exclusive

purpose of monitoring and managing traffic for non-law enforcement purposes and in accordance with 13.08.080.

Data Access

Access to data from the cameras shall be limited to NDOT personnel assigned to the equipment. Some datatypes may contain personally identifiable information (PII). Allowed PII shall mean the image of a license plate, the time and location stamp of an image of a license plate, and the make, model, and color of the vehicle associated with an image of a license plate.

Data Protection

Surveillance technology shall be installed by NDOT employees or NDOT vendors in designated locations. Equipment protection will include physical protection like enclosures and secure mounting, network security, and access controls. Data obtained from cameras shall be kept in a secured facility, subject to local, state, and federal laws.

To ensure that the information obtained through the surveillance technology systems is restricted to what is strictly necessary for the specific purposes, several key steps are taken:

- NDOT clearly defines and documents the specific purposes for which the surveillance technology will be used. This helps in ensuring that data collection and processing are aligned with the purposes in this policy and prevents misuse or overreach.
- NDOT will collect only the data that is necessary for the defined purpose defined in this policy.
- NDOT will implement strict access controls to ensure that only authorized personnel can access the surveillance technology. This includes using personnel-based access controls and ensuring that users have access only to the data necessary for their specific tasks.
- NDOT has developed this Surveillance Usage and Privacy Policy to establish clear data retention that specify how long the surveillance data will be stored. Data will be retained only for as long as necessary to fulfill the defined purposes and will be securely deleted afterwards.
- Where possible, NDOT will anonymize the data to protect individual privacy. Additionally, NDOT will use encryption to protect data both in transit and at rest, ensuring that unauthorized parties cannot access it.

The accuracy of surveillance technology information involving an LPR system and correcting data errors involves these key measures:

- NDOT will Implement validation rules to check the format and consistency of the data as it is collected.
- NDOT will regularly clean the data to remove inaccuracies, duplicates, and inconsistencies.
- NDOT will establish quality control system that includes regular checks, reviews, and validations.
- NDOT will ensure that data from different sources is integrated correctly and consistently.
- NDOT will conduct regular data audits to catch inconsistencies or errors.
- NDOT will implement data security measures to protect data from unauthorized access or corruption.

- NDOT will foster a culture that values data accuracy and consistency through employee training.

Surveillance technology involving an LPR system must follow these monitoring protocols.

- No surveillance data can be viewed unless there is a specific need identified, and then intentional steps must be taken to access the information.
- The data can only be captured and stored locally on the device. There should be no physical way to access the data remotely, in the cloud, or over any network.
- Physical access is only available using dedicated and encrypted handheld remote controller on location.
- All surveillance data must be overwritten within 10 days without ever being viewed by a human asset unless the user intervenes when an incident occurs at the location.

The primary purpose of sharing surveillance technology information is to enhance public safety. Data helps with traffic management, parking violations, illegal dumping violations, fleet management, curb management, and asset management. The process for sharing surveillance technology data involves several steps to ensure accuracy and security. First, the data is collected and validated by the surveillance technology. Once validated, the data is stored in a secure database. **For data involving an LPR system the data will be stored no longer than 10 days.** Authorized personnel can then access this data through a controlled system, requiring login credentials and authorization. If the data is shared, it will be documented in a dissemination log to maintain a record of who accessed the data and for what purpose. This process ensures that the information is used appropriately and can be audited if necessary. NDOT has strict restrictions on sharing surveillance data to protect privacy and ensure data is used only for the purposes defined in this policy. Surveillance technology data is considered "For Official Use Only" and can only be shared with authorized personnel within the department. Unauthorized dissemination of this information can lead to disciplinary actions.

Data Retention of LPR Systems

Data may be printed or downloaded onto an electronic storage device only for the purposes of evidence in a criminal offense or civil traffic or parking offense, subject to a properly issued warrant, subpoena, public records request or court order, or where the department has been instructed to preserve such data by the metropolitan department of law in relation to pending litigation or anticipated litigation. All such data shall be maintained and retained in accordance with applicable state and federal laws.

Data Retention for Surveillance Technology that is NOT an LPR system

Surveillance technology used for NDOT asset management can be beneficial to the department for inventory and condition assessment of Metro Nashville's infrastructure. Surveillance technology used for NDOT's fleet can provide the department with a variety of operational purposes. **When the surveillance information collected does not contain PII data or involve an LPR system or traffic management, NDOT will retain data in accordance with the Metro Records Disposition schedule.**

In addition, The NDOT Traffic Management Center (TMC) facilitates the safe movement of people and goods during congested periods, traffic incidents, planned special events, and severe weather events. The TMC will also support public safety by providing advanced notice of roadway conditions and quickly

responding to traffic signal maintenance issues. Operational safety countermeasures identified in the Nashville Vision Zero Implementation Plan, including coordinated signal timing, leading pedestrian intervals, and pedestrian phasing and cycle lengths to support pedestrian crossings, will also be supported by the TMC. According to **13.08.080:**

NDOT may use technology/equipment to monitor and manage traffic for non-law enforcement purposes. Such technology shall:

1. not save or store data that can be associated with any specific individual or group;
2. not include video that can be paused, rewound, or otherwise viewed in any manner other than real-time;
3. not be monitored by, used by, or acquired by law enforcement personnel for law enforcement purposes, including but not limited to the purposes listed in subsection (E), except for real-time emergency response to support public safety; and
4. be reviewed by the Metropolitan Department of Information Technology Services for data and network security concerns before implementation.

Public Access

Information obtained from surveillance technology shall be made public or deemed exempt from public disclosure pursuant to state or federal law. For public requests for data, NDOT shall confer with metropolitan department of law to determine whether the requested data is exempt from disclosure pursuant to the Tennessee Public Records Act, or is legally required to be disclosed, and shall respond to requests in compliance with applicable laws.

Third-Party Data-Sharing

Data-sharing for the surveillance technology that has PII data shall be prohibited unless for the purposes of evidence in a criminal offense or civil traffic or parking offense, subject to a properly issued warrant, subpoena, public records request or court order, or where the department has been instructed to preserve such data by the metropolitan department of law in relation to pending litigation or anticipated litigation. Unauthorized dissemination of this information can lead to disciplinary actions.

Training

Training for the operation of surveillance technology shall be provided by NDOT personnel to authorized users. All NDOT employees who utilize the systems, or their data shall be provided a copy of this Surveillance Use and Privacy Policy. Training shall include:

- Applicable local, state, and federal laws;
- Applicable policies;
- Functionality of the equipment;
- Authorized and prohibited uses;
- Accessing data;

- Safeguarding password information and data;
- Data sharing policies and procedures;
- Reporting breaches, errors, and other issues;
- Applicable NDOT Standard Operating Procedures

Oversight

NDOT IT division shall have access to the equipment and shall ensure all surveillance technology is utilized in accordance with this policy. An audit log shall be maintained by a NDOT supervisor or administrator for usage of data, which will be reviewed by NDOT administration as it deems necessary, and at least annually, to ensure compliance with this Surveillance Usage and Privacy Policy.