Specification Report – LPR Technology

Sec. 17-5-453: Surveillance Technology Specification Reports.

(a) The Police Department certifies that the information contained in this document reflects the complete and accurate proposed use of the surveillance technology.

(b) This report has been approved by the Chief of Police and received the approval of the Board of Police Commissioners on _____.

(1) Description: Information describing the surveillance technology and its capabilities.

The proposed technology and its capabilities are described as follows:

- Automated detection of license plates utilizing high-speed cameras coupled with proprietary software capable of converting electronic images of license plates into a readable format.
- The digital image can include additional information such as the—

    a. Vehicle's make and model;
    b. The vehicle's driver and passenger(s), and personal property (although this is not the intended use of the LPR technology); and
    c. Distinguishing features (e.g., bumper stickers, damage), and the state of registration.

- Automated comparison of license plate numbers against specified databases.
- In accordance with established parameters, attachment of camera identification, date, time, location information, and direction of travel to the digital image.
- Storage of information on secured servers that meet federal security standards.

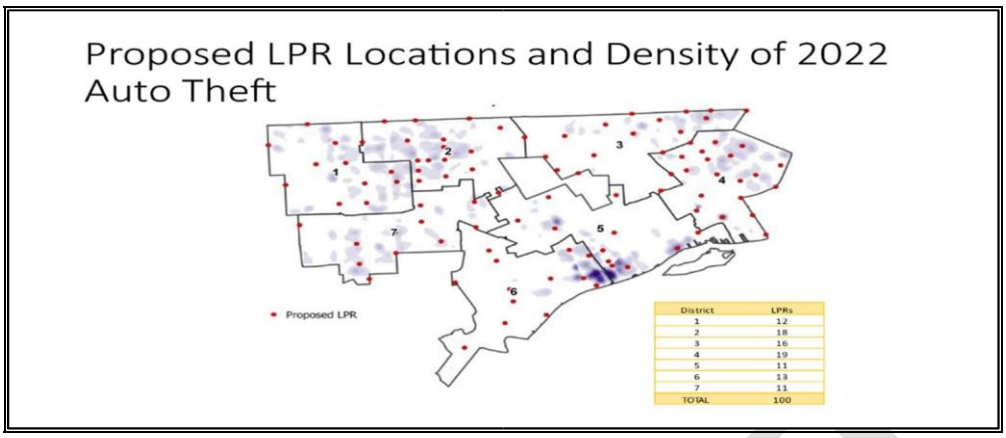
(2) Purpose: Any specific purpose the surveillance technology is intended to advance:

The proposed technology is intended to advance the following lawful purposes:

- Auto-theft prevention and deterrence;
- Apprehension of suspects and fugitives;
- Locating AMBER Alert vehicles;
- Furthering investigations of serious crimes; and
- Other legitimate law enforcement purposes (e.g., crime analysis).

(3) Deployment: If the surveillance technology will not be uniformly deployed or targeted throughout the City, what factors will be used to determine where the technology is deployed or targeted.

- See below:



- DPD identified the deployment based on crime data and logistical considerations.

(4) Fiscal Impact: The fiscal impact of the surveillance technology.

- The contract's total cost is $5 million.
- Of the total contract amount, $3.8 million has been allocated from America Rescue Plan Act (ARPA) funds to cover this contract.

(5) Civil Rights / Liberties Impacts: An assessment identifying with specificity;

(a) Any potential adverse impacts the surveillance technology, if deployed, might have on civil liberties and civil rights; and

- LPR technology does not intrude upon any constitutionally protected areas.
- Misuse of LPR technology or any information collected is strictly prohibited.

(b) What specific, affirmative measures will be implemented to safeguard the public from the potential adverse impacts identified in this section.

- The Police Department will strictly enforce its policies pertaining to the use of LPRs and any information obtained from the technology.

(6) Authorized use: A complete description of the purpose and intended uses of the surveillance technology, including any uses that will be expressly prohibited.

The purpose and intended uses of the proposed technology includes:

- Auto-theft prevention and deterrence;
- Apprehension of suspects and fugitives;
- Locating AMBER Alert vehicles;
- Furthering investigations of serious crimes; and
- Other legitimate law enforcement purposes (e.g., crime analysis).

The following uses of the technology are expressly prohibited:

- Willfully using the LPR for the specific purpose of taking photographs of personal property other than what would typically be expected from normal LPR use;
- Willfully using the LPR for the specific purpose of taking still-photographs of individuals other than what would typically be expected from normal LPR use;
- Traffic enforcement; or
- Track an individual's movements outside of a vehicle.

(7) Data Collection:

(a) What types of surveillance data will be collected, captured, recorded, intercepted, or retained by the surveillance technology;

- LPRs are designed to detect license plates. The system includes a high-speed camera that has the capacity to collect an image of a license plate, information pertaining to the vehicle's make and model, the state of registration, as well as any distinguishing features of the vehicle.

(b) What surveillance data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize the inadvertent collection of data; and

- After careful consideration, the DPD cannot determine any instance or situation where legally protected information may be collected from the proposed technology.
- Although not the intent of the technology, images of the vehicle's driver, passenger, or personal property may be inadvertently collected.

(c) How inadvertently collected surveillance data will be expeditiously identified and deleted.

- After careful consideration, the DPD cannot determine any instance or situation where legally protected information may be collected from the proposed technology.

- The proposed contract provides that the City of Detroit / Police Department owns all of the data collected. In the event protected information is collected through the misuse of the technology, the Police Department will cause for its deletion as soon as feasible.

(8) Data Protection: What safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms.

- The Police Department will comply with FBI / State of Michigan rules pertaining to Criminal Justice Information Systems (CJIS) regulations and other applicable standards and policies to protect data.

(9) Data Retention: Insofar as the privacy of the public can be severely compromised by the long-term storage of mass surveillance data, what rules and procedures will govern the retention of surveillance data, including those governing:

(a) The limited time period, if any, surveillance data will be retained. Such information shall include a statement explaining why the designated retention period is no greater than that which is absolutely necessary to achieve the specific purpose(s) enumerated in the Surveillance Technology Specification Report;

- The DPD will adhere to its Data Retention Policy, which matches the requirements set forth in the corresponding state statute.

(b) The specific conditions that must be met to retain surveillance data beyond the retention period identified pursuant to Subsection (b)(9)(a) of this section; and

- Data will not be retained beyond the retention period except where such information constitutes evidence of a crime related to an open case or a close case where prosecution and / or appeals remain pending.

(c) The process utilized to regularly delete surveillance data after the retention period stated in Subsection (b)(9)(a) of this section has elapsed and the auditing procedures that will be implemented to ensure data is not improperly retained.

- The Police Department's policies and procedures allow for the retention of LPR information for up to one year. However, any hits or reads that were not used in a criminal investigation will be automatically deleted by the system after 30 days for Flock cameras, and 90 days for both Motorola Vigilant, and Genetec cameras. If the Police Department preserves LPR information for use in an investigation, it will fall under the retention and destruction requirements for case files and not under the retention requirements for LPR information. This is a DPD only policy and is in compliance with Michigan law.

(10) Surveillance Data Sharing: If a City department is seeking authorization to share access to surveillance technology or surveillance data with any other governmental agencies, departments, bureaus, divisions, or units, or non-governmental persons or entities in the absence of a judicial warrant or other legal mandate, it shall detail:

(a) Which governmental agencies, departments, bureaus, divisions, or units, or non-governmental persons or entities will be approved for:

i. Surveillance technology sharing to the governmental agency, department, bureau, division, or unit, or non-governmental person or entity, and

ii. Surveillance technology sharing from the governmental agency, department, bureau, division, or unit, or non-governmental person or entity, and

iii. Surveillance data sharing to the governmental agency, department, bureau, division, or unit, or non-governmental person or entity;

(b) Where applicable, the type of information of surveillance data that may be disclosed to the governmental agency, department, bureau, division, or unit, or non-governmental person or entity; and

(c) Where applicable, any safeguards or restrictions that will be imposed on the surveillance technology or data receiving governmental agency, department, bureau, division, or unit, or non-governmental person or entity regarding the use or dissemination of the provided surveillance technology or data;

As of May 17, 2023, the Police Department has entered into Data Sharing Agreements with 31 map - 5/19/23 law enforcement agencies. Under no circumstances are members of the department authorized to share information for the purpose of assessing immigration status or enforcing immigration laws. The DPD will provide a monthly report to the Board of Police Commissioners reflecting the number of law enforcement agencies with whom the Department has data sharing agreements.

(11) Demands for Access to Surveillance Data: What legal standard must be met by government entities or third parties seeking or demanding access to surveillance data.

The Police Department will only share information with government entities or third parties in accordance with a duly authorized data sharing agreement. Under no circumstances is a member of the Police Department authorized to share information for the purpose of assessing immigration status or enforcing immigrations laws.

(12) Auditing and Oversight: What mechanisms will be implemented to ensure the Surveillance Technology Specification Report is followed, including what independent persons or entities will be given oversight authority, if and how regular audits will be conducted, and in the case of the Police Department, also how the Board of Police Commissioners will be involved in the auditing and oversight process.

The primary responsibility of ensuring the Surveillance Technology Specification Report is followed will fall primarily on supervisory and command staff assigned to the Crime Strategies Bureau. The Board of Police Commissioners will continue to serve as the Police Department's civilian oversight body pursuant to the City's Charter.

Upon identifying that protected information has been collected through the misuse of technology, DPD will report the following to the Board of Police Commissioners within 15 days of its discovery:

i. Type of information collected; ii. Date range of the collection;
iii. Extent of impact (i.e., how many person's information was collected);
iv. DPD members who had access to the information; and
v. Date and method of destruction, once it has been destroyed.

On a monthly basis, the Department will provide the Board with a list of members who have access to the LPR technology.

The Department will provide a monthly report of total number of license plate reads for the prior month.

(13) Training: Would specialized training be required in connection with the use of the surveillance technology.

Every member of the Department will receive some degree of training with respect to the technology.

(14) Complaints: What procedures will allow members of the public to register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and how the City department will ensure each question and complaint is responded to in a timely manner.

The policies and procedures of the Detroit Police Department require that upon receiving notice of the desire to file a complaint, a member of the Department must involve a supervisor as soon as possible to receive the complaint. In addition, any citizen may lodge a complaint directly with the Office of the Chief Investigator. Questions regarding the technology may be directed to the Office of the Chief of Police.