13.08.080 Deployment of surveillance or electronic data gathering devices onto public rights-of-way requires metropolitan council approval.

A. For the purposes of this section, the following terms shall be defined as follows:

(1) "Public right-of-way" shall mean any street, avenue, boulevard, highway, sidewalk, alley or public outdoor space which is within the Metropolitan Government of Nashville and Davidson County besides highways that comprise the Dwight D. Eisenhower National System of Interstate and Defense Highways.

(2) "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.

(a) "Surveillance technology" includes, but is not limited to: (i) international mobile subscriber identity (IMSI) catchers and other cell site simulators; (ii) automatic license plate readers; (iii) closed-circuit television cameras; (iv) biometric surveillance technology, including facial, voice, iris, and gait-recognition software and databases; (v) mobile DNA capture technology; (vi) x-ray vans; (vii) video and audio monitoring and/or recording technology, such as surveillance cameras and wide-angle cameras; (viii) surveillance enabled or capable lightbulbs or light fixtures; (ix) tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network; (x) social media monitoring software; (xi) through-the-wall radar or similar imaging technology; (xii) passive scanners of radio networks; (xiii) long-range Bluetooth and other wireless-scanning devices; and (xiv) radio-frequency I.D. (RFID) scanners. The enumeration of surveillance technology examples in this subsection shall not be interpreted as an endorsement or approval of their use.

(b) "Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 13.08.080(A)(2)(a): (i) routine office hardware, such as televisions, computers and printers, that is in widespread public use and will not be used for any surveillance or law enforcement functions; (ii) Parking Ticket Devices (PTDs); (iii) manually operated non-wearable handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (iv) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (v) manually operated technological devices used primarily for internal communications among metropolitan government entities and are not designed to surreptitiously collect surveillance data, such as radios and email systems; (vi) wayfinding technological devices which enable the user to determine global positioning, location within a built environment, or orientation; and (vii) metropolitan government wireless local area networking and metropolitan government databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology.

(c) "Surveillance technology" does not include technology or equipment that collects data in anonymized form or that immediately deletes or destroys non-anonymized collected data.

(3) "Install" or "Installing" shall mean attaching to an existing building, pole, overpass, roadway, sidewalk, natural area, or other structure in a manner that facilitates the permanent or semi-permanent

presence of the applicable device. "Install" or "Installing" shall not mean operating a mobile or portable device intended to be present for a time of limited and discernable length.

(4) "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.

(5) "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.

B. "License plate scanner" shall mean one or more fixed high-speed cameras combined with computer algorithms to convert images of license plates into computer-readable data.

C. Beginning July 1, 2017, approval by the metropolitan council, by a resolution adopted after a public hearing, shall be required prior to any of the following actions by the Metropolitan Government of Nashville or Davidson County, the departments, boards or commissions thereof, or any individual or entity acting upon its behalf:

(1) Installing surveillance technology onto or within the public right-of-way, unless:

(a) the same type of surveillance technology is already in use by the entity; and

(b) the number of new devices does not represent more than a fifty percent increase in the total number of devices of the same type already in use by the department, board, or commission seeking installation, as compared to the number of devices in use at the time of this ordinance's implementation or at the time of the last such approval by the metropolitan council, whichever is more recent.

(2) Entering into an agreement with a private entity to acquire, share or otherwise use surveillance technology or the information it provides if such agreement includes exchange of any monetary or any other form of consideration from any source, including the assessment of any additional fees, interest, or surcharges on unpaid fines or debts absent approval by the metropolitan council;

(3) Accepting state or federal funds or in-kind or other donations for surveillance technology;

(4) Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;

(5) Entering into an intergovernmental agreement regarding the installation of surveillance technology or use of the information it provides within the Dwight D. Eisenhower National System of Interstate and Defense Highways; or

(6) Acquiring or entering into an agreement to acquire surveillance footage or data captured by technology owned by a person or business without the direct consent of that person or business absent a judicial warrant or order to the contrary.

D. The approval by the metropolitan council for any action set forth in subsection 13.08.080(C) above shall be granted only upon the determination that the benefits to the citizens and residents of Nashville and Davidson County outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that,

in the judgment of the metropolitan council, no alternative with a lesser economic cost or impact upon civil rights or civil liberties would be as effective.

E. This section shall not apply to acquisition or use of surveillance technology by or on behalf of law enforcement that is used on a temporary basis for the purpose of a criminal investigation supported by reasonable suspicion, or pursuant to a lawfully issued search warrant, or under exigent circumstances as defined in case law.

F. This section shall not apply to surveillance technology installed for the purpose of securing a building or facility from unlawful entry or unauthorized access.

G. Except as provided in subsection I. of this section, any department of the metropolitan government, either directly or through contractors acting at the department's direction, wishing to acquire or enter into an agreement to acquire license plate scanner (LPR) technology and/or install or operate them onto or within the public rights-of-way, shall comply with the following requirements and restrictions:

1. A usage and privacy policy shall be implemented in order to ensure that the collection, use, maintenance, sharing, and dissemination of LPR information is consistent with respect for individuals' privacy and civil liberties. The usage and privacy policy shall be posted on the department's website, and shall include the following:

(a) i. The authorized purposes for using the LPR system and collecting LPR information, which shall be limited to the following:

(1) investigating and prosecuting felony offenses and criminal offenses associated with violent crimes including gun violence, homicide, and assault; and reckless driving including illegal drag racing activity at speeds in excess of seventy miles per hour;

(2) identification and recovery of stolen vehicles and stolen license plates;

(3) detecting civil traffic or parking offenses;

(4) operating a smart parking or curb management program; and

(5) assisting in missing persons cases including Amber and Silver Alerts.

ii. The use of an LPR system and collection of LPR information is not authorized and shall not be used for any purpose other than those listed in this section. This prohibition includes, but is not limited to the use of LPR for the following:

(1) the general surveillance of any individual;

(2) the identification of a vehicle for the purposes of repossession of the vehicle;

(3) the determination of whether a vehicle's license plate is expired;

(4) the determination of whether a motorist has a valid driver's license; or

(5) the determination of whether a motorist is insured.

iii. An LPR system authorized under this section shall not be capable of facial recognition.

iv. Law Enforcement Agencies, the Parking Enforcement Patrol, NDOT, and their contractors must have reasonable suspicion that a felony offense, or a traffic or parking offenses, has occurred before examining collected license plate reader data that was collected more than one hour prior to the examination. Further, Law Enforcement Officers shall not examine license plate reader data that was collected more than one hour prior to the examination in order to generate reasonable suspicion.

v. Whenever a license plate reader alerts on a plate, law enforcement, before taking any action, must confirm visually that a plate matches the number and state identified in the alert, that the alert is still active by calling dispatch, whether the alert pertains to the registrant of the car and not the car itself, and that the license plate is on the list for one of the authorized purposes listed in this section. Once confirmed, a query shall be initiated in the National Crime Information Center (NCIC) database by authorized individuals.

(b) A description of the employees or contractors who are authorized to use or access the LPR system or to collect LPR information.

(c) A description of the steps taken to restrict the information obtained through the LPR system to that which is strictly necessary to implement the purposes in subsection G.1(a) of this section and limited to the contents of only the license plate and, to the extent possible, excluding identifying information of the driver and passengers.

(d) A description of how the LPR system will be monitored to ensure the security of the information obtained.

(e) The purposes of, process for, and restrictions on the sharing of LPR information to other persons, which must be in accordance with the purposes identified in subsection G.1(a) of this section.

(f) A description of the measures used to ensure the accuracy of LPR information and to correct data errors.

(g) The length of time LPR information will be retained, limited to the terms outlined in subsection G.4 of this section.

2. The installation and maintenance of LPR hardware and software, as well as LPR data access, retention, and security, shall be managed by an LPR custodian ("custodian") designated by the department using the LPR system, who will assign personnel under their command to administer the day to day operation of the LPR system as defined below. The custodian's name shall be provided on the department's website. The custodian shall be the administrator of the LPR system and shall be responsible for developing guidelines and procedures regarding the department's use of its LPR system, including, but not limited to:

(a) Establishing and maintaining reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect LPR information from unauthorized access, destruction, use, modification, or disclosure;

(b) Maintaining a list of the name and job title of all users who are authorized to use or access the department's LPR system;

(c) Developing training requirements for and ensuring training of authorized users on the operations of, and usage and privacy policy for the department's LPR system;

(d) Developing procedures and a regular timetable for conducting audits of LPR system usage, including audits of user searches;

(e) Developing procedures for, and ensuring the proper retention and destruction of, the agency's LPR data;

(f) Ensuring that this policy and its related procedures are posted conspicuously on the department's public website; and

(g) Managing the relationship with the LPR provider, which shall include ensuring that:

i. The provider meets all contractual obligations;

ii. The system is maintained as per Service Level Agreements;

iii. Log retention is adequate; and

iv. Data ownership is clearly understood.

3. Access and use of the department's LPR system is strictly restricted to the authorized users, as outlined below:

   (a) Authorized users must receive appropriate supervisory approval, as determined by the custodian, prior to receiving LPR system access.

   (b) Access shall only be approved for designated personnel whose roles require them to use the LPR system, and LPR system access shall be further limited to those tasks within the employee's job responsibilities. Access shall be limited to no more than ten authorized users per department.

   (c) Personnel authorized to use the department's LPR system as defined in subsection G.3.(b) of this section shall be specifically trained in the system and the usage and privacy policy prior to receiving account access. This training shall include, but not be limited to:

      i. Applicable local, state, and federal laws;

      ii. Applicable policies, including the usage and privacy policy;

      iii. Functionality of the equipment;

      iv. Authorized and prohibited uses;

      v. Accessing data;

      vi. Safeguarding password information and data;

      vii. Data sharing policies and procedures; and

      viii. Reporting breaches, errors, and other issues.

   (d) Authorized user accounts which are inactive for a period of nine months will be disabled automatically. Authorized users with disabled accounts must be retrained in the LPR system, usage, and privacy policies prior to having their accounts reinstated.

   (e) Users found to have used the LPR system without authorization, with improper credentials, or in a manner not authorized by these policies shall have their access immediately revoked and may face disciplinary action in accordance with applicable civil service policies, up to and including termination.

   (f) To the extent consistent with state or federal law, to ensure compliance with the provisions of this section or to investigate complaints of misuse of an LPR or LPRs, the district attorney general, or a designee, or the public defender, or a designee, or the executive director of the community oversight board, or a designee, may examine and audit any LPR, any file used to store LPR data, and any records pertaining to the use of LPRs. If the district attorney general, the public defender, or the executive director of the community oversight board believes that an LPR or LPRs have been used in violation of this section, any of them may send a letter to the metro council requesting suspension of the use of an LPR or LPRs for the purposes of investigation, to prevent ongoing violations, or to deter future violations. The metro council may grant such a request by resolution. Nothing in this section shall be construed as limiting the authority of the district attorney general to prosecute any crime involving LPR. This includes, but is not limited to, tampering with evidence, which is a class C felony punishable under Tennessee law with a term of imprisonment of three to fifteen years and a fine not to exceed ten thousand dollars.

4. (a) LPR data, including but not limited to license plate number, vehicle description, location and date/time stamp shall not be retained for more than ten days, unless it is 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.

(b) Any data unrelated to an ongoing investigation, or pending or anticipated litigation shall be automatically deleted after ten days.

(c) Users who wish to preserve LPR data for longer than ten days shall make a written request to their supervisor including the investigation number and purpose for preservation and, upon approval, such LPR data will be preserved along with a note in the record stating the reason for preservation and related investigation number.

(d) LPR data retained by the metropolitan government shall not include any personally identifiable information, except for Allowed PII.

(e) To the extent permitted by state law, the metropolitan government shall not sell LPR data for any purpose and shall not share any LPR data, except as provided in subsection G.6.

5. The LPR custodian shall perform an audit of the LPR system and its access history on a regular basis, not less than one time per year. The department shall maintain an audit trail of access to the system for a period of not less than three years, which will include the following:

(a) The date and time the information is accessed.

(b) The license plate number or other data elements used to query the LPR system, if such data elements are not deleted per subsection G.4 of this section. Data exempt from deletion under subsection G.4., such as data that will be used as evidence in a felony offense or traffic or parking offense, must be preserved for the audit trail pursuant to this subsection.

(c) The username of the person who accessed the information.

(d) The purpose for accessing the information.

(e) To the extent consistent with state or federal law, access to review the Metropolitan Nashville Police Department audit trail including any audit work papers shall be provided to the district attorney, public defender, and the executive director of the community oversight board, or their respective designees.

6. To the extent consistent with state or federal law, the department's stored LPR data may only be shared with other law enforcement agencies using the following procedures:

(a) The agency making the request for the LPR data shall submit in writing:

i. The name of the agency;

ii. The name and title of the person requesting the information;

iii. The intended purpose of obtaining the information; and

iv. An agreement to adhere to the applicable provisions of this usage and privacy policy.

(b) The request shall be reviewed and approved by the custodian before the requested access is granted.

(c) If the requested search generates results, the custodian or his or her designee must verify that the results are relevant to the request made prior to sharing the LPR data.

(d) The department shall not share any data with any agency that uses that data in a manner broader than allowed by this subsection G.6. Data may only be shared for the purposes outlined in subsection G.1(a).

(e) Records of all approved requests, including a record of which account was used to provide the search results, must be maintained for a period not less than three years.

7. To protect against racial and ethnic bias in the use of LPRs, any time a motor vehicle is stopped based on data analysis performed by an LPR:

   (a) The law enforcement officer who effectuated the stop shall record and provide to their precinct for record keeping and reporting purposes:

      i. The date, time, and precise location of the stop;

      ii. Any investigative or enforcement actions that were taken subsequent to the stop, including without limitation: an arrest; a search of a vehicle, driver, or passenger; the issuance of a new ticket, fine, or fee; or the enforcement of an existing ticket, fine, or fee;

      iii. The self identified race(s) and ethnicities of the driver of the stopped motor vehicle, if voluntarily provided by the driver following the law enforcement officer's request.

   (b) The race and ethnicity identification categories provided to the driver for selection by the law enforcement officer shall be the same as those under present use by the United States Office of Management and Budget (OMB).

   (c) No later than March 1 of each year, the Metropolitan Nashville Police Department (MNPD) shall report to the metropolitan council, and shall make publicly available upon the MNPD website, all of the data collected pursuant to this subsection Section G.7(a), by precinct, from the previous calendar year. The reported data shall include no other personally identifiable information.

   (d) In addition to the reporting requirement in Subsection G.7(c), during the six month pilot program referenced in subsection G.14, the MNPD shall report to the metropolitan council the information required by this subsection G.7(d) every two months. If a resolution is approved to fully implement the MNPD's use of LPR technology, the MNPD shall report such information to the metropolitan council every three months. Each report submitted by the MNPD shall contain the following information, compiled since the end date of its most recent report:

      i. The number of LPRs in use.

      ii. The number of matches made by the LPR, including number of matches read correctly and any misread.

      iii. The number of matches that identified vehicles and individuals sought by law enforcement and that resulted in stops of vehicles or individuals.

      iv. The number of matches that resulted in searches of vehicles and individuals, releases, arrests, or other outcomes.

      v. Other information requested by the metropolitan council by resolution.

8. Failure of an employee to comply with this subsection G shall be grounds for disciplinary action in accordance with applicable civil service policies, up to and including termination.

9. LPR data shall only be disclosed in accordance with state and federal law.

10. LPR data obtained from a privately owned or operated LPR system may be used for the purposes authorized in subsection G.1., provided the data is voluntarily provided by the owners or operators of said LPR systems. The custodian shall develop policies and procedures for requesting, protecting, and retaining this data that are consistent with the intent of subsections G.2., G.3., and G.4.

11. Any device or service necessary to effectuate the provisions of this subsection G shall be procured pursuant to the provisions of Title 4 of the Metropolitan Code of Laws, the Procurement Code. During

the six month pilot program referenced in subsection G.14, the metropolitan government shall not accept a donation of any LPR, LPR device, or LPR service or any donation of funds for the purchase of any LPR, LPR device, or LPR service from any private source. This shall not limit the metropolitan government's ability to accept a grant from a governmental entity. After the conclusion of the pilot program period, and upon the full implementation of the use of LPR, a donation of any LPR, LPR device, or LPR service or any donation of funds for the purchase of any LPR, LPR device, or LPR service shall be subject to the approval of the metropolitan council by resolution, regardless of the value of the donation.

12. An LPR technology deployment policy shall be developed and implemented by the MNPD to help prevent misuse of LPR technology to track and unfairly target vulnerable communities. Placement of fixed LPR technology in the public right-of-way shall be limited to major and collector streets as defined in the Nashville Next Major and Collector Street Plan, and the location of LPR devices shall be distributed equitably across the north, south, east, and west quadrants of the county. Signage shall be placed by any fixed LPR technology to give notice to the public of the use of such technology at a given location. The signage shall be clearly visible and legible to the motoring public and shall state "License Plate Reader Technology In Use".

13. A data verification policy shall be developed and implemented by MNPD to help prevent erroneous and potentially dangerous stops based upon incorrect or outdated information. The policy shall require independent verification of the information yielded from a hot list and real time updating of hot list data, as well as a comparison of the accuracy of the hot list data with the accuracy of the LPR images. Hot lists shall be transferred daily and be capable of updating by an operator/officer in the field. The LPR system, both for fixed and mobile LPR units, shall function in such a manner so as to notify an officer when a license plate on the hot list is observed in real time. Historical LPR data shall be searched to determine the date and time a license plate number contained on a hot list passed a certain camera. For purposes of this subsection G., "hot list" means the list of license plate numbers law enforcement agencies have identified as being relevant for the investigation and/or prosecution of a criminal offense.

14. Prior to the full implementation of a department's LPR system, there shall be a six month pilot program beginning the first day that the LPR system is operational and in use by the department to determine whether the continued use of LPR technology is appropriate. At least two weeks prior to the conclusion of the pilot program period, the department shall submit a report to the council on the efficacy of the program, compliance with the provisions of this section, and any policies implemented in order to carry out the use of the LPR system. This report shall be posted on the department's website. At the end of the six month pilot program, the use of LPR technology by a department shall cease unless the metropolitan council approves the full implementation of the department's use of LPR technology upon adoption of a resolution.

H. Notwithstanding the foregoing, the provisions of this section shall not apply to the Nashville Electric Service, the Metropolitan Nashville Airport Authority, the Metropolitan Development and Housing Agency, and the Metropolitan Transit Authority. Notwithstanding the foregoing, the provisions of this section shall also not apply to the operation of a license plate scanner installed onto or within the public right-of-way that meets each of the following conditions:

   a. The license plate scanner is used solely and exclusively for determining whether a vehicle is violating parking restrictions; and

   b. A specific vehicle's license plate number shall be deleted within thirty minutes of its exit from a monitored parking space, unless that vehicle is suspected of violating parking restrictions for which enforcement action would be appropriate.

I. In addition to the provisions of subsection G. of this section, license plate scanner technology shall be allowed if all of the follow requirements are met:

a. The license plate scanner is used solely and exclusively in conjunction with a vehicle emissions sensor as part of an emissions inspection program authorized under local, state or federal law;

b. The data from the license plate scanner and vehicle emissions sensor is used solely and exclusively for purposes of determining compliance with vehicle emissions standards;

c. A determination by the vehicle emissions sensor that a vehicle identified by the license plate scanner is not in compliance with applicable emissions standards shall not lead to any penalty or punitive action against the registered vehicle owner;

d. No fewer than two such license plate scanners shall be in operation within Davidson County at any given time; and

e. Data that can be used to pair a specific vehicle's license plate number, VIN, or other unique identifier with a specific geographic location shall not be recorded.

(Ord. BL2022-1116 §§ 1, 2, 2022; Ord. BL2022-1114 §§ 1, 2, 2022; Amdt. C to Ord. BL2021-961 § 1, 2022; Amdt. B to Ord. BL2021-961 § 1, 2022; Amdt. A to Ord. BL2021-961 § 1, 2022; Ord. BL2021-961 §§ 1, 2, 2022; Ord. BL2021-679 §§ 1, 2, 2021; Ord. BL2021-646 § 17, 2021; Ord. BL2020-457 § 1, 2020; Amdt. 2 to Ord. BL2017-646 § 1, 2017; Amdt. 1 to Ord. BL2017-646 § 1, 2017; Ord. BL2017-646 § 1, 2017)