

Police Department-operated building or remote command center, where community safety camera network cameras are accessed.

(8) “Donor camera” shall mean any camera owned and maintained by a private entity where the private entity voluntarily elects to participate in the community safety camera network by providing access to common area-facing camera feeds.

(9) “Public safety camera” means a camera owned, installed, and maintained by a governmental entity, including the metropolitan government and any department or agency thereof, which is accessible by the Metropolitan Nashville Police Department (“MNPDP”).

(10) “Public health and safety emergency” means any event or situation that poses a significant threat to the safety and well-being of the general public that would typically require a response by Metro emergency services.

(11) “Residential use” means any parcel that includes a single-family, two-family, or multi-family residence.

Section 2. That Section 13.08.080 is amended by adding a new subsection K as follows:

K. MNPDP may enter into an agreement to participate in a community safety camera network that includes donor cameras, subject to all applicable ordinances. Such participation shall comply with the following additional requirements and restrictions:

1. Community Safety Camera Network Locations and Access

- a. Public safety cameras shall not be installed in a location where there is a reasonable expectation of privacy. A map showing the locations of public safety cameras owned and operated by MNPDP shall be posted on the MNPDP website.
- b. MNPDP shall not have access to a donor camera which:
 - i. views an area where there is a reasonable expectation of privacy;
 - ii. focuses on an area not owned by the operator of the donor camera;
 - iii. views an area other than a common area;
 - iv. is installed upon the property of a residential use and views an area which includes the front door of a residence or the entryway thereto.
- c. MNPDP shall access a donor camera only:
 - i. in a manner accordant with the parameters set by the private entity who owns the donor camera; and
 - ii. only for the purpose of responding to a public health and safety emergency or conducting an audit of the community safety camera network or a component thereof.
- d. Cameras shall only be accessed from within the CSC.

2. System Restrictions

- a. MNPDP shall not record the feed of any camera not owned and operated by MNPDP. All non-evidentiary video footage shall be the property of the camera’s owner.
- b. The community safety camera network shall not be used to identify individuals, or the characteristics thereof, through the use of facial recognition technology. The community safety camera network shall not be used to identify individuals, or the characteristics thereof, through the use of artificial intelligence or machine learning-based solutions, excluding the use of such technologies to make an image more interpretable.

- c. The community safety camera network shall not be used to target, harass, and/or intimidate individuals or groups based solely on actual or perceived characteristics, included but not limited to race, color, religion, sex, age, national origin or ancestry, gender identity, sexual orientation, or disability.
- d. In accordance with MNPD policy provisions regarding the duty to intervene, MNPD employees are required to intervene and stop any MNPD employee from committing an unlawful or improper act as it relates to this subsection K and report such violations.
- e. MNPD shall not share video from donor cameras with any individual, group, or entity for a purpose not outlined in subsection K.1(c).

3. Policies Required

- a. MNPD shall develop and publish on its website a policy addressing authorized access to and use of the community safety camera network which includes:
 - i. Criteria for designating personnel who may access the community safety camera network.
 - ii. Training standards for such personnel. Those standards shall, at a minimum, include applicable laws, policies, procedures, authorized and prohibited uses, and duty to intervene.
 - iii. Procedures for disciplinary action for failure to adhere to the policy.
- b. MNPD shall develop and publish on its website a policy for retention of videos obtained through the community safety camera network which includes:
 - i. Acknowledgment that MNPD shall not set retention policies for donor camera video saved on systems belonging to private entities.
 - ii. Reiteration of existing MNPD policies for retention of video from cameras owned and operated by MNPD.
 - iii. Acknowledgment that video that has evidentiary value shall be collected in accordance with established MNPD procedures and legal requirements.
- c. MNPD shall post a log of all changes to these policies which includes a clear indication of what language was added, removed, or replaced as well as the date of the change.

4. System Audits and Reporting

- a. The commander of the CSC shall perform an audit of the community safety camera network on a regular basis, not less than one time per quarter. The department shall maintain an audit trail of access to donor cameras for a period of not less than three years, which will include the following:
 - i. The date and time that a donor camera is accessed.
 - ii. The username of the person who accessed the donor camera.
 - iii. The purpose for accessing the donor camera.
 - iv. The outcome of the incident which caused the accessing of a donor camera.
- b. No later than September 1 of each year, MNPD shall report to the metropolitan council, and shall publish on the MNPD website, the following data from the previous fiscal year:
 - i. The number of donor cameras registered as part of the camera safety network.

- ii. The number of incidents in which one or more donor cameras were accessed.
- iii. Outcomes of incidents which caused the accessing of donor cameras.
- c. Any violation of this ordinance or material violations of the community safety camera network access or use policies shall be reported to the mayor and metropolitan council within seven days of discovery.

5. Contract Requirements

- a. Any contract to effectuate the provisions of this subsection K shall be procured pursuant to the provisions of Title 4 of the Metropolitan Code of Laws, the Procurement Code.
- b. Any such contract shall include a termination clause which immediately terminates the contract upon written notice after a finding by MNPD or metropolitan department of law, or a vote of the metropolitan council, that one or more of the following occurred:
 - i. A change in applicable law, including but not limited to federal or state statute, regulation, ordinance, executive order, or directive, that would permit the use of the community safety camera network in a manner not specifically authorized in the agreement approved by the metropolitan council and applicable ordinances and policies.
 - ii. The use of the community safety camera network in a manner that the culpable individual knew or should have known was not specifically authorized by the metropolitan council under the contract and applicable ordinances and policies in place on the date of execution.

- 6. A public hearing shall be required to be held at a metropolitan council meeting prior to passage of an ordinance amending this subsection K.

Section 3. This ordinance shall take effect from and after its adoption, the welfare of The Metropolitan Government of Nashville and Davidson County requiring it.

Analysis

This ordinance, as amended, amends Metropolitan Code of Laws Section 13.08.080 regarding the use of a community safety camera network. The ordinance would add a new subsection authorizing the Metropolitan Nashville Police Department (“MNPD”) to enter into an agreement to participate in a community safety camera network to provide an integrated video management system to provide access to live or recorded videos.

Any participation in a community safety camera network must comply with the requirements and restrictions in the ordinance.

Public safety cameras, to be defined as cameras owned, installed, and maintained by a governmental entity and accessible by MNPD, could not be installed in a location where there is a reasonable expectation of privacy. MNPD would be required to post online a map of the locations of public safety cameras owned and operated by MNPD.

Donor cameras, to be defined as a camera owned and maintained by a private entity where the private entity voluntarily elects to participate in the community safety camera network, could not be accessed by MNPD if the donor camera: (1) views an area where there is a reasonable expectation of privacy, (2) focuses on an area not owned by a donor camera’s operator, (3) views an area other than a common area, (4) is installed

upon a residential property and views an area including a front door or entry way of the residence, or (5) is installed upon the property of a multifamily residential use and focuses on an area other than a parking lot, parking garage, or other outdoor common area.

MNPD could only access a donor camera (1) in a manner consistent with limitations set by the private entity who owns the donor camera and (2) for the purpose of responding to a public health and safety emergency or auditing the community safety camera network. The ordinance defines “public health and safety emergency” as “any event or situation that poses a significant threat to the safety and well-being of the general public that would typically require a response by Metro emergency services.” Cameras could only be accessed from within the Community Safety Center. In addition, MNPD would not have access to live video from a donor camera if located upon the property of a solely residential use.

Video from donor cameras could not be shared by MNPD with any individual, group, or entity except (1) in a manner consistent with limitations set by the private entity who owns the donor camera and (2) for the purpose of responding to a public health and safety emergency or auditing the community safety camera network.

MNPD would be prohibited from recording a camera feed that it does not own or operate, and the camera’s owner would retain ownership of all non-evidentiary video footage. The ordinance would prohibit a community safety camera network from being used to identify individuals through facial recognition technology, artificial intelligence, or machine learning-based solutions, except for technologies that would make an image more interpretable. In addition, the network could not use artificial intelligence, machine learning-based solutions, or any other artificial mechanism to capture conversations through automatic lip reading. The community safety camera network could not be used to target, harass, or intimidate individuals based entirely because of actual or perceived characteristics, including race, color, religion, sex, age, national origin or ancestry, gender identity, sexual orientation, or disability. In accordance with MNPD policy provisions regarding the duty to intervene, where video collected from the network captures any MNPD employee utilizing excessive or unlawful force, the video must be preserved and provided to the MNPD Office of Professional Accountability and the District Attorney General. The ordinance would require MNPD employees to intervene and stop unlawful or improper use of a community safety camera network consistent with MNPD policy regarding a duty to intervene.

MNPD would be required to develop and publish online a policy that addresses authorized access to and use of the community safety camera network. The policy must include criteria for designating personnel who may access the community safety camera network, training standards for those personnel, and procedures for disciplinary action for failure to adhere to the policy. A separate policy would also be developed and published online regarding the retention of videos obtained through the community safety camera network and must acknowledge that MNPD cannot set retention policies for donor camera video saved on systems that belong to private entities, reiterate existing MNPD policies for retention of video from MNPD cameras, and acknowledge that video with evidentiary value must be collected in accordance with established MNPD procedures and legal requirements. MNPD would be required to post a log of all changes to these policies and indicate what language was added, removed, or replaced as well as the date of the change.

Each officer responsible for accessing donor cameras would be required to document in writing (1) the date, time, and circumstance of each instance of access a donor camera and (2) a narrative detailing the purpose for accessing the donor camera.

The community safety center's commander would be required to regularly perform an audit of the community safety camera network at least once per quarter. An audit trail of access to donor camera must be kept for at least three years and include dates and times when a donor camera is access, the username of the person that accessed the donor camera, the purpose for accessing the donor camera, and the outcome of the incident which caused the camera to be accessed.

The ordinance would further require MNPD to publish and provide an annual report to the Metropolitan Council no later than September 1 of each year. The report would be required include the number of donor cameras registered, the number of incidents which required access to a donor camera, and the outcome to incidents requiring donor camera access for the previous fiscal year. Any violations of the ordinance or access or use policies would be required to be reported to the Mayor and the Council within seven days of discovery. The Mayor or the Metropolitan Council would be authorized to hire an independent firm to conduct an audit of the records created and kept under the ordinance.

Any contract to effectuate a community safety camera network would be required to be procured consistent with the Procurement Code of the Metropolitan Code of Laws. Any contract would be required to include a termination clause that would immediately end the contract upon written notice after a finding from MNPD or the Department of Law or a vote from the Council that the following has occurred: a change in applicable law would permit the use of the community safety camera network in a manner not specifically authorized in the agreement and applicable ordinances and policies, or the community safety camera network was used in a manner that the culpable individual knew or should have known was not specifically authorized by the metropolitan council under the contract and applicable ordinances and policies in place when the agreement was executed.

A public hearing would be required before an ordinance amending this new subsection is passed by the Council.