LOCAL LAWS
OF
THE CITY OF NEW YORK
FOR THE YEAR 2025

No. 56

Introduced by Council Members Won, Brewer, Farías, Marte, Rivera, Cabán, Hudson, Banks, Salaam, Krishnan, Williams, Ossé, Ayala, Sanchez, Avilés, Nurse, Hanif, Abreu, De La Rosa, Louis, Gutiérrez and Mealy.

A LOCAL LAW

To amend the administrative code of the city of New York, in relation to police department transparency in the use of surveillance technology

Be it enacted by the Council as follows:

Section 1. Section 14-188 of the administrative code of the city of New York, as added by local law number 65 for the year 2020, is amended to read as follows:

§ 14-188 Annual surveillance reporting and evaluation. a. Definitions. As used in this section, the following terms have the following meanings:

Surveillance technology. The term "surveillance technology" means equipment, software, or systems capable of, or used or designed for, collecting, retaining, processing, or sharing audio, video, location, thermal, biometric, or similar information, that is operated by or at the direction of the department. Surveillance technology does not include:

1. routine office equipment used primarily for departmental administrative purposes;

2. parking ticket devices;

3. technology used primarily for internal department communication; or

4. cameras installed to monitor and protect the physical integrity of city infrastructure.

Surveillance technology impact and use policy. The term “surveillance *technology* impact and use policy” means a written document that includes the following information:

1. a description of the capabilities of a surveillance technology;

2. rules, processes and guidelines issued by the department regulating access to or use of such surveillance technology as well as any prohibitions or restrictions on use, including whether the department obtains a court authorization for such use of a surveillance technology, and, if so, the specific type of court authorization sought;

3. safeguards or security measures designed to protect information collected by such surveillance technology from unauthorized access, including but not limited to the existence of encryption and access control mechanisms;

4. policies and/or practices relating to the retention, access, and use of data collected by such surveillance technology;

5. policies and procedures relating to access or use of the data collected through such surveillance technology by members of the public;

6. [whether] *names of all* entities outside the department, *including local government entities, state government entities, federal government entities, or private entities, that* have access to the information and data collected by such surveillance technology, including: (a) [whether the entity is a local governmental entity, state governmental entity, federal governmental entity or a private entity, (b)] the type of information and data that may be disclosed [by] *to* each such entity, and [(c) any] *(b) the specific* safeguards or restrictions imposed by the department on *each* such entity regarding the use or dissemination of the information *and data* collected by such surveillance technology. *This paragraph shall not apply to public disclosures of information and data collected by such surveillance technology, including but not limited to disclosures made pursuant*

to the freedom of information law or information provided in connection with press or media inquiries;

7. whether any training is required by the department for an individual to use such surveillance technology or access information collected by such surveillance technology;

8. a description of internal audit and oversight mechanisms within the department to ensure compliance with the surveillance technology impact and use policy governing the use of such surveillance technology;

9. *(a)* any tests or reports regarding the health and safety effects of the surveillance technology; and *(b) any known physical safety hazards of the surveillance technology, physical safety hazards identifiable by manufacturer warnings, or published academic research regarding physical safety hazards, or a statement that no such hazards have been identified after a search for relevant information; and*

10. any potentially disparate impacts of the *surveillance technology and* surveillance technology impact and use policy on any protected groups as defined in the New York city human rights law.

b. Publication of surveillance technology impact and use policy. The department shall propose a surveillance technology impact and use policy and post such proposal on the department's website, at least 90 days prior to the use of any new *and distinct* surveillance technology.

1. Surveillance technologies shall be considered distinct for the purposes of this section where they differ in function. Examples of distinct surveillance technologies shall include but not be limited to remote-controlled aerial cameras, cameras attached to autonomous robots, fixed cameras, and cameras equipped with facial recognition. If a surveillance technology product identified pursuant to paragraph 3 of this subdivision is included in more than one impact and use

policy, the department shall provide a public particularized explanation of why the department takes the position that such product is not a distinct surveillance technology that requires the proposal of a new impact and use policy.

2. The department shall update an existing impact and use policy to describe a new, but not distinct, surveillance technology, which has the same function but substantially differs in form or has a different manufacturer or product name.

3. A surveillance technology impact and use policy shall identify the manufacturer and product name of each surveillance technology that is addressed by the impact and use policy, including the specific capability and component of the surveillance technology that is addressed by such policy if such product is listed in more than one such policy, provided that where disclosure of such manufacturer or product name would endanger the safety of the public or officers or interfere with an active investigation, and where such information is not already publicly known, the department shall not publicly disclose such manufacturer or product name, or both, to the extent such disclosure would pose such a risk. In such circumstances, the department shall provide a public particularized explanation, specific to the relevant surveillance technology, of why such disclosure would endanger the safety of the public or officers or interfere with an active investigation; provided further that the department shall not be required to include any details or information in such description that would endanger the safety of the public or officers or interfere with an active investigation. Nothing in this paragraph shall be construed to permit the department to withhold disclosure of manufacturers or product names from the commissioner of investigation. As part of the audit pursuant to section 803 of the New York city charter, the commissioner of investigation may state whether any manufacturer or product name was improperly withheld.

c. Existing surveillance technology. For existing surveillance technology as of the effective date of the local law that added this section, the department shall propose a surveillance technology impact and use policy and post such proposal on the department's website within 180 days of such effective date.

d. Addendum to surveillance technology impact and use policies. When the department seeks to acquire or acquires enhancements to surveillance technology or uses such surveillance technology for a purpose or in a manner not previously disclosed through the surveillance technology impact and use policy, the department shall provide an addendum to the existing surveillance technology impact and use policy describing such enhancement or additional use. *Routine patches, firmware or software updates, and hardware lifecycle replacements that do not materially alter surveillance functions or capabilities do not require an addendum to or new surveillance technology impact and use policy.*

e. Upon publication of any proposed surveillance technology impact and use policy, the public shall have 45 days to submit comments on such policy to the commissioner.

f. The commissioner shall consider public comments and provide the final surveillance technology impact and use policy to the speaker and the mayor, and shall post it on the department's website no more than 45 days after the close of the public comment period established by subdivision e of this section.

g. Internal tracking. Within 270 days of the effective date of the local law that added this subdivision, the department shall create an internal tracking system that complies with this subdivision.

(1) Such tracking system shall document each instance in which the department provides an external entity with data collected by the department using a surveillance technology, including

the name of the entity and the date that such data was provided. This paragraph shall not apply to (i) public disclosures, including but not limited to disclosures made pursuant to the freedom of information law, made in connection with press or media inquiries, or provided to academic or research organizations; and (ii) disclosures made to other government entities, provided that such system shall document each instance in which the department provides data to United States immigration and customs enforcement and United States customs and border protection, except data that is disclosed for the purposes of furthering a criminal investigation to any task force in which the United States immigration and customs enforcement or United States customs and border protection participates, where the department does not maintain sole control or supervision over such data.

(2) the department shall develop an internal tracking system listing each local, state, or federal government agency that has direct access to data collected by the department using surveillance technology and the extent of the data to which the agency has direct access and for which dates the agency has direct access.

h. Intergovernmental data sharing. The department shall develop a policy regarding the circumstances under which any local, state, or federal government agency has access to data collected by the department using surveillance technology.

(1) Such policy shall identify the circumstances under which such data can be shared or must be shared, the criteria for sharing, and which data would be shared with which agencies under which circumstances. The department may develop one policy for all such data for all local, state, or federal government agencies, provided that, to the extent that certain categories of data or certain local, state, or federal government agencies receive data under different standards or in different circumstances, such differences shall be noted.

(2) Such policy shall identify the local, state or federal government agencies that the department knows participate in any task force that has access to such data, provided that such policy need not specify the policy of the entity that maintains such data for such task force that governs the sharing of such data with such agencies.

(3) Such policy shall identify whether the department has any actual knowledge that law enforcement agencies with access to such data share such data with United States immigration and customs enforcement or United States customs and border protection and under which circumstances. Such policy shall also identify which measures, if any, the department takes to minimize the risk of such data being used for civil immigration enforcement.

i. Within 270 days of the local law that added this section and annually thereafter, the department shall conduct a review of evidence of physical safety hazards posed by surveillance technologies used by the department, including but not limited to evaluations by experts in the field, and shall include any identified physical hazards in the surveillance technology impact and use policy. Such review shall be conducted in such a way as to be reasonably calculated to uncover any prominent and readily available research and analysis of the physical safety of the surveillance technology and shall include internet-wide keyword searches.

§ 2. This local law takes effect immediately, provided that within 270 days of the effective date of this local law, the New York city police department shall update and publish new surveillance technology impact and use policies to bring existing impact and use policies into compliance with this local law, including by updating and publishing new surveillance technology impact and use policies to disclose information on surveillance technologies that were not new at the time of the enactment of this local law but which would have resulted in additional disclosures had this local law been in effect at the time that such surveillance technologies were new.

THE CITY OF NEW YORK, OFFICE OF THE CITY CLERK, s.s.:

I hereby certify that the foregoing is a true copy of a local law of The City of New York, passed by the Council on April 10, 2025 and returned unsigned by the Mayor on May 12, 2025.

MICHAEL M. McSWEENEY, City Clerk, Clerk of the Council.

CERTIFICATION OF CORPORATION COUNSEL

I hereby certify that the form of the enclosed local law (Local Law No. 56 of 2025, Council Int. No. 480-A of 2024) to be filed with the Secretary of State contains the correct text of the local law passed by the New York City Council, presented to the Mayor, and neither approved nor disapproved within thirty days thereafter.

SPENCER FISHER, Acting Corporation Counsel.