



Legislation Text

File #: Int 0690-2026, **Version:** *

Int. No. 690

By Council Members Brewer, Hudson, Fariás, Won and Louis

A Local Law to amend the administrative code of the city of New York, in relation to requiring comprehensive reporting and oversight of the use of surveillance technology for law enforcement purposes by certain agencies

Be it enacted by the Council as follows:

Section 1. Subdivision a of section 14-188 of the administrative code of the city of New York, as amended by local law number 56 for the year 2025, is amended by adding a new definition of “responder agency” in alphabetical order, to read as follows:

Responder agency. The term “responder agency” means the fire department, department of correction, department of probation, department of investigation, department of finance, or office of emergency management.

§ 2. Subdivision h of section 14-188 of the administrative code of the city of New York, as amended by local law number 56 for the year 2025, is amended to read as follows:

h. Intergovernmental data sharing. 1. 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.] (a) 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.] (b) 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.] (c) 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.

2. The commissioner shall not use the surveillance technology, or data developed from the surveillance technology, of any responder agency, nor shall the commissioner request that a responder agency use such technology for the purposes of a department law enforcement action, when doing so would circumvent a department surveillance technology impact and use policy or a policy established pursuant to section 14-188.1.

§ 3. Chapter 1 of title 14 of the administrative code of the city of New York is amended by adding a new section 14-188.2 to read as follows:

§ 14-188.2 Surveillance reporting and evaluation for other law enforcement and first responder agencies. a. Definitions. For purposes of this section, the following terms have the following meanings:

Agency head. The term “agency head” means the commissioner or head of any responder agency.

Facial recognition technology impact and use policy. The term “facial recognition impact and use policy” means a written document that includes the following information:

1. a description of the capabilities of the facial recognition technology;
2. a description of the responder agency’s use of facial recognition technology;
3. restrictions placed on access and use of facial recognition technology by personnel of the responder

agency, including procedures for supervisory approval and internal oversight to safeguard against improper use of such technology;

4. guidelines related to the modification of an original image used for comparison analysis by facial recognition technology;

5. whether any training is required by the responder agency for an individual to use such facial recognition technology;

6. a description of internal audit and oversight mechanisms within the responder agency to ensure compliance with the facial recognition technology impact and use policy governing the use of such facial recognition technology; and

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

IUP. The term “IUP” means a facial recognition technology impact and use policy or surveillance technology impact and use policy developed by a responder agency, as applicable.

Responder agency. The term “responder agency” has the same meaning as given in subdivision a of section 14-188.

Surveillance technology. The term “surveillance technology” has the same meaning as given in subdivision a of section 14-188.

Surveillance technology impact and use policy. The term “surveillance technology impact and use policy” has the same meaning as given in subdivision a of section 14-188.

b. Publication of surveillance and facial recognition policies of responder agencies. 1. Prospective surveillance technology. Each agency head shall propose an IUP and post any such proposal on such responder agency’s website at least 90 days prior to the use of any new and distinct surveillance technology.

(a) Surveillance technologies shall be considered distinct for the purposes of this section where they differ in function. Examples of distinct surveillance technologies include, but are not 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 subparagraph (iii) of this paragraph is included in more than one IUP, the agency head of the responder agency proposing such policy shall provide a public, particularized explanation of why that agency head takes the position that such product is not a distinct surveillance technology that requires the proposal of a new IUP.

(b) When a responder agency procures a new, but not distinct, surveillance technology, the agency head of such responder agency shall update an existing IUP to describe such technology when such technology has the same function but substantially differs in form or has a different manufacturer or product name.

(c) An IUP shall identify the manufacturer and product name of each surveillance technology that is addressed by the IUP, 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.

(d) A single IUP for a surveillance technology with facial recognition functionality may include all information required for both a surveillance technology impact and use policy and a facial recognition impact and use policy.

2. Existing surveillance technology. For any existing surveillance technology as of the effective date of the local law that added this section that a responder agency possesses, the agency head of such responder agency shall propose an IUP and post such proposal on the responder agency's website within 180 days of such effective date.

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

4. Public comment and publication of impact and use policies. (a) Upon publication of any proposed IUP as required under paragraph 1 or 2 of this subdivision, the public shall have 45 days to submit comments on such policy to the agency head.

(b) The agency head shall consider public comments and provide the final IUP to the commissioner, the speaker of the council, and the mayor, and shall post it on the website of the responder agency no more than 45 days after the close of the public comment period established by subparagraph (a) of this paragraph.

5. Collaboration on impact and use policies. (a) When multiple responder agencies procure the same surveillance technology, the agency heads of such responder agencies may collaborate to produce a single IUP addressing impacts and uses by all such agencies. Any IUP produced via collaboration shall still be subject to the requirements of paragraphs 1, 2, 3, and 4 above.

(b) When a responder agency acquires surveillance technology that would require an addendum to an IUP created under this paragraph, or a responder agency develops new uses for an existing surveillance technology not covered by an IUP created pursuant to this paragraph, the agency head of such responder agency may separately update the IUP. Such addendum would apply solely to the responder agency that developed the additional technology or additional use.

d. Intergovernmental data sharing. 1. Policies for local, state, and federal agencies generally. The agency head of each responder agency shall develop policies regarding the circumstances under which any local, state, or federal government agency has access to data collected by such responder agency using surveillance technology.

(a) Such policies 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 agency head of each responder agency 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.

(b) Such policies shall identify the local, state, or federal government agencies that the agency head of a responder agency 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.

(c) Such policies shall identify whether the agency head of a responder agency 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 policies shall also identify which measures, if any, the agency head of a responder agency takes to minimize the risk of such data being used for civil immigration enforcement.

2. Policies regarding use of data from the police department. An agency head shall not use or request the use of surveillance technology, or data developed from the surveillance technology, of the department if doing so would violate a policy developed pursuant to paragraph 1 of this subdivision.

§ 4. This local law takes effect immediately.

JMF
LS #17268/17384/20125/20126/20130
2/13/2026 11:46 AM