STATE OF NEW YORK

6776

2019-2020 Regular Sessions

IN SENATE

October 11, 2019

Introduced by Sen. HOYLMAN -- read twice and ordered printed, and when printed to be committed to the Committee on Rules

AN ACT to amend the executive law, in relation to prohibiting facial recognition technology to be used in connection with an officer camera; and providing for the repeal of such provisions upon expiration thereof

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The executive law is amended by adding a new section 837-u to read as follows:

§ 837-u. Use of facial recognition in connection with an officer camera prohibited. 1. Definitions. For the purposes of this section, the following terms shall have the following meanings:

(a) "Biometric data" means a physiological, biological or behavioral characteristic that can be used, singly or in combination with each other or with other information, to establish individual identity.

(b) (i) "Facial recognition or other biometric surveillance" means either of the following, alone or in combination:

(1) An automated or semi-automated process by which a person is identified or attempted to be identified based on the characteristics of their face or based on their biometric data, including identification of known or unknown individuals or groups; and/or

(2) An automated or semi-automated process that generates, or assists in generating, surveillance information about an individual based on the characteristics of an individual's face or based on biometric data.

(ii) "Facial recognition or other biometric surveillance" shall not include the use of an automated or semi-automated process for the purpose of redacting a recording for release or disclosure outside a police agency to protect the privacy of a subject depicted in the recording, if the process does not generate or result in the retention of any biometric data or surveillance information.

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD13977-01-9

(c) "Facial recognition or biometric surveillance system" means any computer software or application that performs facial recognition or other biometric surveillance.

(d) "Police agency", "police officer" and "peace officer" shall have the same meanings as defined under section eight hundred thirty-five of this article.

(e) "Officer camera" means a body-worn camera or similar device that records or transmits images or sound and is attached to the body or clothing of, or carried by, a police officer or peace officer.

(f) "Surveillance information" means either of the following, alone or in combination:

(i) Any information about a known or unknown individual, including but not limited to, a person's name, date of birth, gender or criminal background; and/or

(ii) Any information derived from biometric data, including but not limited to, assessments about an individual's sentiment, state of mind or level of dangerousness.

(g) "Use" means either of the following, alone or in combination:

(i) The direct use of a facial recognition or biometric surveillance system by a police agency, police officer or peace officer; and/or

(ii) A request by a police officer or peace officer that a police agency or other third party use a facial recognition or biometric surveillance system on behalf of the requesting entity.

2. No police agency, police officer or peace officer shall install, activate or use any facial recognition or biometric surveillance system in connection with an officer camera or data collected by an officer camera.

3. In addition to any other sanctions, penalties or remedies provided by law, a person may bring an action for equitable or declaratory relief in a court of competent jurisdiction against a police agency, police officer or peace officer that violates this section.

4. This section does not preclude a police agency, police officer or peace officer from using a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification if this use is lawful and does not generate or result in the retention of any biometric data or surveillance information.

§ 2. The executive law is amended by adding a new section 234 to read as follows:

§ 234. Use of facial recognition in connection with an officer camera prohibited. 1. Definitions. For the purposes of this section, the following terms shall have the following meanings:

(a) "Biometric data" means a physiological, biological or behavioral characteristic that can be used, singly or in combination with each other or with other information, to establish individual identity.

(b) (i) "Facial recognition or other biometric surveillance" means either of the following, alone or in combination:

(1) An automated or semi-automated process by which a person is identified or attempted to be identified based on the characteristics of their face or based on their biometric data, including identification of known or unknown individuals or groups; and/or

(2) An automated or semi-automated process that generates, or assists in generating, surveillance information about an individual based on the characteristics of an individual's face or based on biometric data.

(ii) "Facial recognition or other biometric surveillance" shall not include the use of an automated or semi-automated process for the purpose of redacting a recording for release or disclosure outside the

division of state police to protect the privacy of a subject depicted in the recording, if the process does not generate or result in the retention of any biometric data or surveillance information.

(c) "Facial recognition or biometric surveillance system" means any computer software or application that performs facial recognition or other biometric surveillance.

(d) "Officer camera" means a body-worn camera or similar device that records or transmits images or sound and is attached to the body or clothing of, or carried by, a member of the state police.

(e) "Surveillance information" means either of the following, alone or in combination:

(i) Any information about a known or unknown individual, including but not limited to, a person's name, date of birth, gender or criminal background; and/or

(ii) Any information derived from biometric data, including but not limited to, assessments about an individual's sentiment, state of mind or level of dangerousness.

(f) "Use" means either of the following, alone or in combination:

(i) The direct use of a facial recognition or biometric surveillance system by a member of the state police; and/or

(ii) A request by a member of the state police that a police agency or other third party use a facial recognition or biometric surveillance system on behalf of the requesting entity.

2. No member of the state police shall install, activate or use any facial recognition or biometric surveillance system in connection with an officer camera or data collected by an officer camera.

3. In addition to any other sanctions, penalties or remedies provided by law, a person may bring an action for equitable or declaratory relief in a court of competent jurisdiction against a member of the state police that violates this section.

4. This section does not preclude a member of the state police from using a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification if this use is lawful and does not generate or result in the retention of any biometric data or surveillance information.

§ 3. This act shall take effect on the ninetieth day after it shall have become a law and shall expire and be deemed repealed 5 years after such date.