STATE OF NEW YORK

7572

IN SENATE

January 27, 2020

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

AN ACT to amend the executive law, in relation to prohibiting the use of biometric surveillance technology by law enforcement; establishing the biometric surveillance regulation task force; and providing for the repeal of certain provisions upon expiration thereof

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

Section 1. Legislative intent. The legislature finds and declares the following:

(a) The use of biometric surveillance technology has been largely unregulated by all levels of government in the United States to date, allowing its unfettered use by private entities, government, and law enforcement with little to no requirements or restrictions relating to use, data retention, privacy protections, and use of information derived from such systems in law enforcement investigations. In New York, this lack of regulation and oversight has led to concerning practices by law enforcement, such as including sealed mugshots and arrest photos of juveniles in facial recognition databases and running photos of celebrity lookalikes through facial recognition software to attempt to identify potential suspects.

(b) Studies of currently available biometric surveillance technology demonstrate that such technology's consistency and accuracy can vary widely based on age, gender, sex, race, and other factors, and has been found to be particularly inaccurate when used on women, young people, and people of color.

(c) These accuracy concerns are particularly troubling in the context of this technology's ongoing and increasing use by law enforcement. New York's law enforcement should not rely on technology that has demonstrated accuracy issues, as such practice risks the wrongful targeting, interrogation, detention, or even conviction of an innocent person based on erroneous data.

(d) The largest U.S. supplier of police body cameras has publicly stated that this technology "is not currently reliable enough to

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

LBD14547-04-0

ethically justify its use," and other major companies working on this technology have chosen not to offer it for general use until concerns about the technology's accuracy are resolved.

(e) In addition to accuracy concerns, the continuous use of this technology for broad, untargeted surveillance purposes constitutes an unacceptable mass violation of privacy and could chill New Yorkers' right to free speech and freedom of assembly.

(f) In order to protect the personal data, civil rights, civil liberties, and due process rights of all New Yorkers, the use of this technology by law enforcement should not currently be permitted, and more study and research should be conducted into the impacts of this technology before determining whether it should be authorized for use, and under what circumstances such use should be permitted.

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

§ 837-u. Use of biometric surveillance systems prohibited. 1. Definitions. For the purposes of this section, the following terms shall have the following meanings:

(a) "Biometric information" means any measurable physiological, biological or behavioral characteristics that are attributable to an individual person, including facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other physical characteristics that can be used, singly or in combination with each other or with other information, to establish individual identity. Examples of biometric information include, but are not limited to, fingerprints, handprints, retina and iris patterns, DNA sequence, voice, gait, and facial geometry.

(b)(i) "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 their biometric information, 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 their biometric information.

(ii) "Biometric surveillance" shall not include the use of an automated or semi-automated process for the purposes of:

(1) 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 information or surveillance information;

(2) the state DNA identification index in accordance with the provisions of section nine hundred ninety-five-c of this chapter; or

(3) the taking, submission, and processing of fingerprints for the state identification bureau, provided that such taking, submission and processing is explicitly authorized by law.

(c) "Biometric surveillance system" means any computer software or application that performs biometric surveillance, but does not include the state DNA identification index or the fingerprint identification portion of the state automated biometric identification system.

(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) "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, aggregated location data, or criminal background; and/or

(ii) Any information derived from biometric information, 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 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 biometric surveillance system on behalf of the requesting entity.

2. No police agency, police officer or peace officer shall acquire, possess, access, install, activate or use any biometric surveillance system, or any biometric information or surveillance information derived from the use of a biometric surveillance system by any other entity, while in the course of their job duties or with regard to any information obtained, processed, or accessed in the course of those duties.

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:

(a) lawfully using a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification if a police officer or peace officer has reasonable cause to arrest such person or to issue to and serve upon such person an appearance ticket, provided that any biometric or surveillance information retained through the use of such device may be used solely for the purposes permitted in this paragraph or other purposes explicitly authorized by law;

(b) accessing DNA comparisons between forensic evidence and designated offenders, as defined in subdivision seven of section nine hundred ninety-five of this chapter, through the state DNA identification index pursuant to section nine hundred ninety-five-c of this chapter;

(c) accessing fingerprint comparisons using the statewide automated biometric identification system for the purpose of routine booking or crime scene comparisons; or

(d) using any lawfully installed security system that processes biometric information solely for the purpose of verifying the identity of members, officers, employees, agents, or other affiliated staff of the police agency in order to determine whether such persons are permitted to access information, goods, materials, areas, or other possessions or property belonging to or under the custody of the police agency.

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

§ 234. Use of biometric surveillance systems prohibited. 1. Definitions. For the purposes of this section, the following terms shall have the following meanings:

(a) "Biometric information" means any measurable physiological, biological or behavioral characteristics that are attributable to an individual person, including facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other physical characteristics that can be used, singly or in combination with each other or with other information, to estab-

lish individual identity. Examples of biometric information include, but are not limited to, fingerprints, handprints, retina and iris patterns, DNA sequence, voice, gait, and facial geometry.

(b) (i) "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 their biometric information, 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 their biometric information.

(ii) "Biometric surveillance" shall not include the use of an automated or semi-automated process for the purposes of:

(1) redacting a recording for release or disclosure outside the 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 information or surveillance information;

(2) the state DNA identification index in accordance with the provisions of section nine hundred ninety-five-c of this chapter; or

(3) the taking, submission, and processing of fingerprints for the state identification bureau, provided that such taking, submission and processing is explicitly authorized by law.

(c) "Biometric surveillance system" means any computer software or application that performs biometric surveillance.

(d) "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, aggregated location data, or criminal background; and/or

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

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

(i) The direct use of a 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 biometric surveillance system on behalf of the requesting entity.

2. No member of the state police shall acquire, possess, access, install, activate or use any biometric surveillance system, or any biometric information or surveillance information derived from the use of a biometric surveillance system by any other entity, while in the course of their job duties or with regard to any information obtained, processed, or accessed in the course of those duties.

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:

(a) lawfully using a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification if a member of the state police has reasonable cause to arrest such person or to issue to and serve upon such person an appearance ticket, provided that any biometric or surveillance information retained through the use of such device may be used solely for the

purposes permitted in this paragraph or other purposes explicitly authorized by law;

(b) accessing DNA comparisons between forensic evidence and designated offenders, as defined in subdivision seven of section nine hundred ninety-five of this chapter, through the state DNA identification index pursuant to section nine hundred ninety-five-c of this chapter;

(c) accessing fingerprint comparisons using the statewide automated biometric identification system for the purpose of routine booking or crime scene comparisons; or

(d) using any lawfully installed security system that processes biometric information solely for the purpose of verifying the identity of members, officers, employees, agents, or other affiliated staff of the state police in order to determine whether such persons are permitted to access information, goods, materials, areas, or other possessions or property belonging to or under the custody of the state police.

§ 4. Biometric surveillance regulation task force. 1. (a) There is hereby established the task force on the regulation of biometric surveillance, which shall consist of twelve members as follows:

(a) the commissioner of the division of criminal justice services or his or her designee;

(b) the superintendent of state police or his or her designee;

(c) the commissioner of the New York city police department or his or her designee; and

(d) three members appointed by the governor, two members appointed by the temporary president of the senate, two members appointed by the speaker of the assembly, one member appointed by the minority leader of the senate, and one member appointed by the minority leader of the assembly, each of which shall have expertise and experience related to at least one of the following fields, disciplines, or areas:

(i) data privacy and data security;

(ii) civil rights, civil liberties, and due process and procedural rights;

(iii) the use and function of both existing and emerging biometric surveillance technology;

(iv) legal representation of low-income individuals and/or tenants; or

(v) criminal defense.

(b) The chairperson of the task force shall be one of the governor's appointees, whom the governor shall so designate.

(c) The task force shall meet as often as is necessary, but no less than three times per year, and at the call of the chairperson. Meetings may be held via teleconference. All members shall be provided with written notice reasonably in advance of each meeting with date, time and location of such meeting.

(d) Any vacancies on the task force shall be filled in the manner provided for in the initial appointment.

(e) Members of the task force shall receive no compensation for their services but shall be reimbursed for their actual expenses incurred in the performance of their duties in the work of the task force.

(f) The task force is authorized to hold public hearings and meetings and to consult with any relevant stakeholders it deems appropriate or necessary to seek assistance, data, or other information that will enable the task force to carry out its powers and duties.

(g) The division of criminal justice services shall provide the task force with such facilities, assistance and data as will enable the task force to carry out its powers and duties. Additionally, all other agencies of the state or subdivisions thereof may, at the request of the

chairperson of the task force, provide the task force with such facilities, assistance, and data as will enable the task force to carry out its powers and duties.

2. The task force shall:

(a) Examine the current and proposed use of biometric surveillance systems, as such term is defined pursuant to section 837-u of the executive law, by governments and/or law enforcement, both in the United States and abroad;

(b) Examine current and proposed laws, rules, regulations, programs, and policies relating to the use of biometric surveillance systems;

(c) Examine currently available biometric surveillance systems or similar technology, and evaluate their effectiveness, efficacy, and accuracy, provided that such evaluation shall include the use of representative datasets according to targeted populations, and disaggregated testing for demographic subgroups by age, gender identity, and race;

(d) Evaluate the potential benefits and harms of the use of biometric surveillance systems, taking into account and analyzing the impact of the use of such systems on minorities, women, young people, seniors, lesbian, gay, bisexual, transgender, and gender-nonconforming individuals, and individuals with disabilities;

(e) Evaluate whether law enforcement should be permitted to use biometric surveillance systems, and if it is the judgment of the task force that such use should be permitted, the task force shall propose a comprehensive framework of recommendations for legislation, regulations and standards regarding the use of such systems by law enforcement, including, but not limited to:

(i) permissible uses and purposes for use of biometric surveillance systems by law enforcement;

(ii) prohibited uses and purposes for use of biometric surveillance systems by law enforcement;

(iii) minimum standards for accuracy that biometric surveillance systems must achieve in order to be authorized for use by law enforcement, and auditing requirements to ensure compliance with those standards;

(iv) standards for use, management, and protection of information derived from the use of biometric surveillance systems by law enforcement, including, but not limited to data retention, sharing, access, and audit trails;

(v) rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity;

(vi) training requirements for law enforcement personnel authorized to use biometric surveillance systems;

(vii) procedures to address instances in which a person is wrongfully targeted, arrested or interrogated based on inaccurate information derived from the use of a biometric surveillance system; and

(viii) disclosure requirements for broad public transparency as well as discovery procedures.

3. (a) No sooner than January 1, 2024, and no later than January 1, 2025, the task force shall transmit a report to the governor, the temporary president of the senate, the speaker of the assembly, the minority leader of the senate, and the minority leader of the assembly detailing its findings and recommendations pursuant to subdivision two of this section.

(b) No later than ten days after the task force transmits such report to the governor, the temporary president of the senate, the speaker of the assembly, the minority leader of the senate, and the minority leader

of the assembly, the division of criminal justice services shall make such report available on its website.

§ 5. This act shall take effect immediately, provided that section four of this act shall expire and be deemed repealed 60 days after transmission of the report of the findings and recommendations of the task force to the governor, the temporary president of the senate, the speaker of the assembly, the minority leader of the senate, and the minority leader of the assembly, as provided in paragraph (a) of subdivision 3 of section four of this act. Provided, however, that the commissioner of the department of criminal justice services shall notify the legislative bill drafting commission upon the transmission of the report of the findings of the task force, as provided in paragraph (a) of subdivision 3 of section four of this act, in order that the commission may maintain an accurate and timely effective data base of the official text of the laws of the state of New York in furtherance of effectuating the provisions of section 44 of the legislative law and section 70-b of the public officers law.