STATE OF NEW YORK

10036

IN ASSEMBLY

April 29, 2022

Introduced by M. of A. GONZALEZ-ROJAS -- read once and referred to the Committee on Governmental Operations

AN ACT to amend the executive law, in relation to banning the use of biometric data by certain state agencies

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 170-f to read as follows:

§ 170-f. Use of biometric recognition technology prohibited. 1. For the purposes of this section, the following terms shall have the following meanings:

(a) "Biometric data" shall mean any measurable physiological, biological or behavioral characteristics that are attributable to a person, including facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, genetic characteristics, vocal characteristics or thermal characteristics that can be used, either singularly or in combination with each other or can be paired or combined with other information, to establish individual identity.

(b) "Biometric recognition technology" shall mean either or both (i) any automated or semi-automated process or processes by which a person is identified or attempted to be identified based on their biometric data, including identification of known or unknown individuals or groups; and/or (ii) any automated or semi-automated process or processes that generates or assists in generating, information about any individual based on their biometric data, including but not limited to emotion, affect, or behavior detection.

(c) "Equity impact assessment" shall mean an audit and report addressing, at a minimum, the following:

(i) Evaluation of potential benefits, harms, and impacts on persons or groups of persons who are protected from discrimination as set forth in article fifteen of this chapter, including specific considerations based on a person's ethnic and racial background. Such evaluation shall also include, although not be limited to the disproportionate collection and use of such technology on ethnic and racial minorities in New York

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

LBD14858-01-2

state, the disproportionate use of such technology in locations where ethnic and racial minorities reside, and the disproportionate representation of particular ethnic and racial minorities in any underlying datasets used to develop and/or implement such technology;

(ii) Evaluation of the efficacy and accuracy of the biometric recognition technology, including the accuracy of such technology in identifying persons who belong to a group or groups protected from discrimination as set forth in article fifteen of this chapter and a description of the methodology of such evaluation, including whether such evaluation involved a controlled or real-world study;

(iii) Steps taken or planned by the state or local agency to address and to reduce any disparities or inaccuracies identified in subparagraphs (i) or (ii) of this paragraph, along with the state or local agency's reasoning for continuing to use the biometric recognition technology despite the disparate impact or inaccuracy;

(iv) Procedures to address and challenge false results and protective measures and preventative checks against such occurrences, and an assessment of the adequacy of such procedures;

(v) What protections are put in place for due process, privacy, free speech and association, and racial, gender, and religious equity;

(vi) Whether the state or local agency considered a less-intrusive alternative prior to utilizing the technology, and if so, a description of such an explanation for why such alternative was not ultimately used; and

(vii) Costs associated with the use of the technology and storage of relevant data, including any maintenance costs, administrative costs or other costs incurred.

2. (a) Unless explicitly required by other provisions of state law, it shall be unlawful for any state or local agency to:

(i) Acquire, access, or use any biometric recognition technology or any biometric data; or

(ii) Direct the use of any biometric recognition technology or the collection of any biometric data by a third party.

(b) To the extent that any state or local agency is currently using any biometric recognition technology or collecting any biometric data and such use or collection is not otherwise required by any other provision of state law, such state or local agency shall immediately stop using such technology or data.

(c) Nothing in this subdivision shall be construed to prevent a state or local agency or an employee of a state or local agency from:

(i) Obtaining or possessing any device equipped with biometric recognition technology, provided such device is being held as evidence and the state or local agency or the employee of such agency does not access or use the biometric recognition technology of such device;

(ii) Acquiring, accessing, or using any biometric recognition technology on a device owned by the state or local agency or an employee of such agency, for the sole purpose of user authentication of agency employees provided that the agency does not access or use such biometric recognition technology for any other purpose other than user authentication and provided that no biometric data of individuals not employed by such agency are intentionally entered, retained, or processed by such technology;

(iii) Accessing or using a technology or service not owned by the state or local agency or an employee of such agency but which is operated by a third party, provided that the agency or an employee of the agency does not process, use, request, or retain any information created

by the biometric recognition technology and that no biometric data of individuals not employed by such agency are intentionally entered, or processed by such technology; or

(iv) Acquiring, accessing, or using an automated or semi-automated process for the purpose of redacting a recording for release or disclosure outside the state or local agency to protect the privacy of a subject depicted in the recording, provided that the process does not generate or result in the retention of any biometric data.

(d) Nothing in this subdivision shall be construed to prevent a public health or public education agency from acquiring, accessing, or using biometric recognition technology or biometric data for purposes related to public health, research, or education, provided that such biometric recognition technologies or biometric data are not shared with a law enforcement agency.

(e) Nothing in this subdivision shall be construed to prevent a state or local agency from:

(i) Collecting a genetic or fingerprint sample or samples that are abandoned at the scene of an alleged criminal offense and is not collected from the person of a criminal suspect; or

(ii) Collecting genetic samples from an individual who is alleged to be the victim of a crime and who consents to such collection.

3. On or before May first, two thousand twenty-two, and annually thereafter, any state or local agency using or acquiring for use biometric recognition technology or biometric data as explicitly required by any other provision of state law shall:

(a) 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 each biometric recognition technology or type of biometric data it intends to acquire, access, use, collect or analyze. Each state or local agency required to file a report shall also publish such report on the state or local agency's website. Such report shall also include, but not be limited to, the following:

(i) The type of biometric data;

(ii) The type and vendor of biometric recognition technology;

(iii) The state law that, in the state or local agency's view, explicitly requires such acquisition, access, use, collection, or analysis or biometric recognition technology or biometric data;

(iv) The time period, if any, that the biometric data will be retained and the reasons the specific biometric data will be retained for during the designated time period;

(v) Whether any biometric data will be shared with another individual or entity and if so, with what individuals or entities it will be shared, and whether explicit authorization exists for such data to be shared;

(vi) The risk of an unauthorized access to or breach of retained biometric data, safeguards or security measures designed to mitigate any such risk, and appropriate consequences for failure to adhere to such safeguards or security measures in the event of unauthorized access or a breach; and

(vii) Related to any unauthorized breaches of retained biometric data since May first of the previous year, a description of: (1) any such breaches; (2) the results of any completed investigations of any such breaches; (3) any attempts to notify anyone impacted by any such breach or whose biometric data may have been unlawfully accessed; and

(4) any actions the state or local agency has taken to address any breaches.

(b) Transmit an equity impact assessment as defined in subdivision one of this section 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 well as publishing such assessment to the state agency, police agency, or the state police's own web page.

(c) Transmit an equity impact assessment as defined in subdivision one of this section to the civil rights bureau of the office of the attorney general, which shall review such assessment and make recommendations or take other action as may be appropriate with respect to any disparity or inaccuracy identified in such assessment.

§ 2. The executive law is amended by adding a new section 235 to read as follows:

§ 235. Use of biometric recognition technology prohibited. 1. For the purposes of this section the following terms shall have the following meanings:

(a) "Biometric data" shall mean any measurable physiological, biological or behavioral characteristics that are attributable to a person, including facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, genetic characteristics, vocal characteristics, thermal characteristics that can be used, either singularly or in combination with each other or can be paired or combined with other information, to establish individual identity.

(b) "Biometric recognition technology" shall mean either or both (i) any automated or semi-automated process or processes by which a person is identified or attempted to be identified based on their biometric data, including identification of known or unknown individuals or groups; and/or (ii) any automated or semi-automated process or processes that generates or assists in generating, information about any individual based on their biometric data, including but not limited to emotion, affect, or behavior detection.

(c) "Equity impact assessment" shall mean an audit and report addressing, at a minimum, the following:

(i) Evaluation of potential benefits, harms, and impacts on persons or groups of persons who are protected from discrimination as set forth in article fifteen of this chapter, including specific considerations based on a person's ethnic and racial background. Such evaluation shall also include, although not be limited to the disproportionate collection and use of such technology on ethnic and racial minorities in New York state, the disproportionate use of such technology in locations where ethnic and racial minorities reside, and the disproportionate representation of particular ethnic and racial minorities in any underlying datasets used to develop and/or implement such technology;

(ii) Evaluation of the efficacy and accuracy of the biometric recognition technology, including the accuracy of such technology in identifying persons who belong to a group or groups protected from discrimination as set forth in article fifteen of this chapter, and a description of the methodology of such evaluation, including whether such evaluation involved a controlled or real-world study;

(iii) Steps taken or planned by the division of state police to address and to reduce any disparities or inaccuracies identified in subparagraphs (i) or (ii) of this paragraph, along with the agency's reasoning for continuing to use the biometric recognition technology despite the disparate impact or inaccuracy;

(iv) Procedures to address and challenge false results and protective measures and preventative checks against such occurrences, and an assessment of the adequacy of such procedures;

(v) What protections are put in place for due process, privacy, free speech and association, and racial, gender, and religious equity;

(vi) Whether the division of state police considered a less-intrusive alternative prior to utilizing the technology, and if so, a description of such an explanation for why such alternative was not ultimately used; and

(vii) Costs associated with the use of the technology and storage of relevant data, including any maintenance costs, administrative costs or other costs incurred.

2. (a) Unless explicitly required by other provisions of state law, it shall be unlawful for any member of the division of state police to:

(i) Acquire, access, or use any biometric recognition technology or any biometric data; or

(ii) Direct the use of any biometric recognition technology or the collection of any biometric data by a third party.

(b) To the extent that the division of state police is currently using any biometric recognition technology or collecting any biometric data and such use or collection is not otherwise required by any other provision of state law, the division of state police shall immediately stop using such technology or data.

(c) Nothing in this subdivision shall be construed to prevent the state police or a member of the state police from:

(i) Obtaining or possessing any device equipped with biometric recognition technology, provided such device is being held as evidence and the division of state police or the employee of the division of state police does not access or use the biometric recognition technology of such device;

(ii) Acquiring, accessing, or using any biometric recognition technology on a device owned by the division of state police or an employee of the division of state police, for the sole purpose of user authentication of agency employees provided that the division of state police does not access or use such biometric recognition technology for any other purpose other than user authentication and provided that no biometric data of individuals not employed by the division of state police are intentionally entered, retained, or processed by such technology;

(iii) Accessing or using a technology or service not owned by the division of state police or an employee of the division of state police but which is operated by a third party, provided that the division of state police or an employee of the division of state police does not process, use, request, or retain any information created by the biometric recognition technology and that no biometric data of individuals not employed by the division of state police are intentionally entered, or processed by such technology; or

(iv) Acquiring, accessing, or using 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, provided that the process does not generate or result in the retention of any biometric data.

(d) Nothing in this subdivision shall be construed to prevent the division of state police or members of the division of state police from:

(i) Collecting a genetic or fingerprint sample or samples that are abandoned at the scene of an alleged criminal offense and is not collected from the person of a criminal suspect; or

(ii) Collecting genetic samples from an individual who is alleged to be the victim of a crime and who consents to such collection.

3. On or before May first, two thousand twenty-two and annually thereafter, any division of state police using or acquiring for use biometric recognition technology or biometric data as explicitly required by any other provision of state law shall:

(a) 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 each biometric recognition technology or type of biometric data it intends to acquire, access, use, collect or analyze. Each division of state police required to file a report shall also publish such report on the division of state police's website. Such report shall also include, but not be limited to, the following:

(i) The type of biometric data;

(ii) The type and vendor of biometric recognition technology;

(iii) The state law that, in the division of state police's view, explicitly requires such acquisition, access, use, collection, or analysis or biometric recognition technology or biometric data;

(iv) The time period, if any, that the biometric data will be retained and the reasons the specific biometric data will be retained for during the designated time period;

(v) Whether any biometric data will be shared with another individual or entity and if so, with what individuals or entities it will be shared, and whether explicit authorization exists for such data to be shared;

(vi) The risk of an unauthorized access to or breach of retained biometric data, safeguards or security measures designed to mitigate any such risk, and appropriate consequences for failure to adhere to such safeguards or security measures in the event of unauthorized access or a breach; and

(vii) Related to any unauthorized breaches of retained biometric data since May first of the previous year, a description of: (1) any such breaches; (2) the results of any completed investigations of any such breaches; (3) any attempts to notify anyone impacted by any such breach or whose biometric data may have been unlawfully accessed; and (4) any actions the agency has taken to address any breaches.

(b) Transmit an equity impact assessment as defined in subdivision one of this section 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 well as publishing such assessment to the state agency, police agency, or the division of state police's own web page.

(c) Transmit an equity impact assessment as defined in subdivision one of this section to the civil rights bureau of the office of the attorney general, which shall review such assessment and make recommendations or take other action as may be appropriate with respect to any disparity or inaccuracy identified in such assessment.

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

§ 837-x. Use of biometric recognition technology prohibited. 1. For the purposes of this section the following terms shall have the following meanings:

(a) "Biometric data" shall mean any measurable physiological, biological or behavioral characteristics that are attributable to a person, including facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, genetic characteristics, vocal characteristics, thermal characteristics that can be used, either singularly or in combination with each other or can be paired or combined with other information, to establish individual identity.

(b) "Biometric recognition technology" shall mean either or both (i) any automated or semi-automated process or processes by which a person is identified or attempted to be identified based on their biometric data, including identification of known or unknown individuals or groups; and/or (ii) any automated or semi-automated process or processes that generates or assists in generating, information about any individual based on their biometric data, including but not limited to emotion, affect, or behavior detection.

(c) "Equity impact assessment" shall mean an audit and report addressing, at a minimum, the following:

(i) Evaluation of potential benefits, harms, and impacts on persons or groups of persons who are protected from discrimination as set forth in article fifteen of this chapter, including specific considerations based on a person's ethnic and racial background. Such evaluation shall also include, although not be limited to the disproportionate collection and use of such technology on ethnic and racial minorities in New York state, the disproportionate use of such technology in locations where ethnic and racial minorities reside, and the disproportionate representation of particular ethnic and racial minorities in any underlying datasets used to develop and/or implement such technology;

(ii) Evaluation of the efficacy and accuracy of the biometric recognition technology, including the accuracy of such technology in identifying persons who belong to a group or groups protected from discrimination as set forth in article fifteen of this chapter, and a description of the methodology of such evaluation, including whether such evaluation involved a controlled or real-world study;

(iii) Steps taken or planned by the agency to address and to reduce any disparities or inaccuracies identified in subparagraphs (i) or (ii) of this paragraph, along with the police agency, police officer or peace officer's reasoning for continuing to use the biometric recognition technology despite the disparate impact or inaccuracy;

(iv) Procedures to address and challenge false results and protective measures and preventative checks against such occurrences, and an assessment of the adequacy of such procedures;

(v) What protections are put in place for due process, privacy, free speech and association, and racial, gender, and religious equity;

(vi) Whether the police agency, police officer or peace officer considered a less-intrusive alternative prior to utilizing the technology, and if so, a description of such an explanation for why such alternative was not ultimately used; and

(vii) Costs associated with the use of the technology and storage of relevant data, including any maintenance costs, administrative costs or other costs incurred.

2. (a) Unless explicitly required by other provisions of state law, it shall be unlawful for any police agency, police officer or peace officer to:

(i) Acquire, access, or use any biometric recognition technology or any biometric data; or

(ii) Direct the use of any biometric recognition technology or the collection of any biometric data by a third party.

(b) To the extent that any police agency, police officer or peace officer is currently using any biometric recognition technology or collecting any biometric data and such use or collection is not otherwise required by any other provision of state law, such police agency, police officer or peace officer shall immediately stop using such technology or data.

(c) Nothing in this subdivision shall be construed to prevent a police agency, police officer or peace officer from:

(i) Obtaining or possessing any device equipped with biometric recognition technology, provided such device is being held as evidence and the police agency, police officer or peace officer does not access or use the biometric recognition technology of such device; or

(ii) Acquiring, accessing, or using any biometric recognition technology on a device owned by the police agency, police officer or peace officer for the sole purpose of user authentication of police agency employees, police officers or peace officers provided that the police agency does not access or use such biometric recognition technology for any other purpose other than user authentication and provided that no biometric data of individuals not employed by the police agency are intentionally entered, retained, or processed by such technology; or

(iii) Accessing or using a technology or service not owned by the police agency, police officer or peace officer but which is operated by a third party, provided that the police agency, police officer or peace officer does not process, use, request, or retain any information created by the biometric recognition technology and that no data of individuals not employed by the police agency are intentionally entered, or processed by such technology; or

(iv) Acquiring, accessing, or using an automated or semi-automated process for the purpose of redacting a recording for release or disclosure outside the police agency to protect the privacy of a subject depicted in the recording, provided that the process does not generate or result in the retention of any biometric data.

(d) Nothing in this subdivision shall be construed to prevent a police agency, police officer or peace officer from:

(i) Collecting a genetic or fingerprint sample or samples that are abandoned at the scene of an alleged criminal offense and is not collected from the person of a criminal suspect; or

(ii) Collecting genetic samples from an individual who is alleged to be the victim of a crime and who consents to such collection.

3. On or before May first, two thousand twenty-two and annually thereafter, any police agency using or acquiring for use biometric recognition technology or biometric data as explicitly required by any other provision of state law shall:

(a) 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 each biometric recognition technology or type of biometric data it intends to acquire, access, use, collect or analyze. Each police agency required to file a report shall also publish such report on the police agency's website. Such report shall also include, but not be limited to, the following:

(i) The type of biometric data;

(ii) The type and vendor of biometric recognition technology;

(iii) The state law that, in the police agency's view, explicitly requires such acquisition, access, use, collection, or analysis or biometric recognition technology or biometric data;

(iv) The time period, if any, that the biometric data will be retained and the reasons the specific biometric data will be retained for during the designated time period;

(v) Whether any biometric data will be shared with another individual or entity and if so, with what individuals or entities it will be shared, and whether explicit authorization exists for such data to be shared;

(vi) The risk of an unauthorized access to or breach of retained biometric data, safeguards or security measures designed to mitigate any such risk, and appropriate consequences for failure to adhere to such safeguards or security measures in the event of unauthorized access or a breach; and

(vii) Related to any unauthorized breaches of retained biometric data since May first of the previous year, a description of: (1) any such breaches; (2) the results of any completed investigations of any such breaches; (3) any attempts to notify anyone impacted by any such breach or whose biometric data may have been unlawfully accessed; and (4) any actions the agency has taken to address any breaches.

(b) Transmit an equity impact assessment as defined in subdivision one of this section 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 well as publishing such assessment to the state agency, police agency, or the state police's own web page.

(c) Transmit an equity impact assessment as defined in subdivision one of this section to the civil rights bureau of the office of the attorney general, which shall review such assessment and make recommendations or take other action as may be appropriate with respect to any disparity or inaccuracy identified in such assessment.

§ 4. This act shall take effect immediately.