

# 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:

1 Section 1. The executive law is amended by adding a new section 170-f  
2 to read as follows:

3 § 170-f. Use of biometric recognition technology prohibited. 1. For  
4 the purposes of this section, the following terms shall have the follow-  
5 ing meanings:

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

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

21 (c) "Equity impact assessment" shall mean an audit and report address-  
22 ing, at a minimum, the following:

23 (i) Evaluation of potential benefits, harms, and impacts on persons or  
24 groups of persons who are protected from discrimination as set forth in  
25 article fifteen of this chapter, including specific considerations based  
26 on a person's ethnic and racial background. Such evaluation shall also  
27 include, although not be limited to the disproportionate collection and  
28 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

1 state, the disproportionate use of such technology in locations where  
2 ethnic and racial minorities reside, and the disproportionate represen-  
3 tation of particular ethnic and racial minorities in any underlying  
4 datasets used to develop and/or implement such technology;

5 (ii) Evaluation of the efficacy and accuracy of the biometric recogni-  
6 tion technology, including the accuracy of such technology in identify-  
7 ing persons who belong to a group or groups protected from discrimi-  
8 nation as set forth in article fifteen of this chapter and a description  
9 of the methodology of such evaluation, including whether such evaluation  
10 involved a controlled or real-world study;

11 (iii) Steps taken or planned by the state or local agency to address  
12 and to reduce any disparities or inaccuracies identified in subpara-  
13 graphs (i) or (ii) of this paragraph, along with the state or local  
14 agency's reasoning for continuing to use the biometric recognition tech-  
15 nology despite the disparate impact or inaccuracy;

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

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

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

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

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

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

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

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

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

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

45 (ii) Acquiring, accessing, or using any biometric recognition technol-  
46 ogy on a device owned by the state or local agency or an employee of  
47 such agency, for the sole purpose of user authentication of agency  
48 employees provided that the agency does not access or use such biometric  
49 recognition technology for any other purpose other than user authentica-  
50 tion and provided that no biometric data of individuals not employed by  
51 such agency are intentionally entered, retained, or processed by such  
52 technology;

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

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

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

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

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

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

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

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

26 (a) Transmit a report to the governor, the temporary president of the  
27 senate, the speaker of the assembly, the minority leader of the senate,  
28 and the minority leader of the assembly detailing each biometric recog-  
29 nition technology or type of biometric data it intends to acquire,  
30 access, use, collect or analyze. Each state or local agency required to  
31 file a report shall also publish such report on the state or local agen-  
32 cy's website. Such report shall also include, but not be limited to, the  
33 following:

34 (i) The type of biometric data;

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

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

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

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

46 (vi) The risk of an unauthorized access to or breach of retained biom-  
47 etric data, safeguards or security measures designed to mitigate any  
48 such risk, and appropriate consequences for failure to adhere to such  
49 safeguards or security measures in the event of unauthorized access or a  
50 breach; and

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

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

3 (b) Transmit an equity impact assessment as defined in subdivision one  
4 of this section to the governor, the temporary president of the senate,  
5 the speaker of the assembly, the minority leader of the senate, and the  
6 minority leader of the assembly as well as publishing such assessment to  
7 the state agency, police agency, or the state police's own web page.

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

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

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

18 (a) "Biometric data" shall mean any measurable physiological, biolog-  
19 ical or behavioral characteristics that are attributable to a person,  
20 including facial characteristics, fingerprint characteristics, hand  
21 characteristics, eye characteristics, genetic characteristics, vocal  
22 characteristics, thermal characteristics that can be used, either singu-  
23 larly or in combination with each other or can be paired or combined  
24 with other information, to establish individual identity.

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

33 (c) "Equity impact assessment" shall mean an audit and report address-  
34 ing, at a minimum, the following:

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

45 (ii) Evaluation of the efficacy and accuracy of the biometric recogni-  
46 tion technology, including the accuracy of such technology in identify-  
47 ing persons who belong to a group or groups protected from discrimi-  
48 nation as set forth in article fifteen of this chapter, and a  
49 description of the methodology of such evaluation, including whether  
50 such evaluation involved a controlled or real-world study;

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

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

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

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

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

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

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

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

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

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

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

31 (ii) Acquiring, accessing, or using any biometric recognition technol-  
32 ogy on a device owned by the division of state police or an employee of  
33 the division of state police, for the sole purpose of user authentica-  
34 tion of agency employees provided that the division of state police does  
35 not access or use such biometric recognition technology for any other  
36 purpose other than user authentication and provided that no biometric  
37 data of individuals not employed by the division of state police are  
38 intentionally entered, retained, or processed by such technology;

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

47 (iv) Acquiring, accessing, or using an automated or semi-automated  
48 process for the purpose of redacting a recording for release or disclo-  
49 sure outside the division of state police to protect the privacy of a  
50 subject depicted in the recording, provided that the process does not  
51 generate or result in the retention of any biometric data.

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



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

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

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

10 (a) Transmit a report to the governor, the temporary president of the  
11 senate, the speaker of the assembly, the minority leader of the senate,  
12 and the minority leader of the assembly detailing each biometric recog-  
13 nition technology or type of biometric data it intends to acquire,  
14 access, use, collect or analyze. Each division of state police required  
15 to file a report shall also publish such report on the division of state  
16 police's website. Such report shall also include, but not be limited to,  
17 the following:

18 (i) The type of biometric data;

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

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

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

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

30 (vi) The risk of an unauthorized access to or breach of retained biom-  
31 etric data, safeguards or security measures designed to mitigate any  
32 such risk, and appropriate consequences for failure to adhere to such  
33 safeguards or security measures in the event of unauthorized access or a  
34 breach; and

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

41 (b) Transmit an equity impact assessment as defined in subdivision one  
42 of this section to the governor, the temporary president of the senate,  
43 the speaker of the assembly, the minority leader of the senate, and the  
44 minority leader of the assembly as well as publishing such assessment to  
45 the state agency, police agency, or the division of state police's own  
46 web page.

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

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

54 § 837-x. Use of biometric recognition technology prohibited. 1. For  
55 the purposes of this section the following terms shall have the follow-  
56 ing meanings:

1 (a) "Biometric data" shall mean any measurable physiological, biolog-  
2 ical or behavioral characteristics that are attributable to a person,  
3 including facial characteristics, fingerprint characteristics, hand  
4 characteristics, eye characteristics, genetic characteristics, vocal  
5 characteristics, thermal characteristics that can be used, either singu-  
6 larly or in combination with each other or can be paired or combined  
7 with other information, to establish individual identity.

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

16 (c) "Equity impact assessment" shall mean an audit and report address-  
17 ing, at a minimum, the following:

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

28 (ii) Evaluation of the efficacy and accuracy of the biometric recogni-  
29 tion technology, including the accuracy of such technology in identify-  
30 ing persons who belong to a group or groups protected from discrimi-  
31 nation as set forth in article fifteen of this chapter, and a  
32 description of the methodology of such evaluation, including whether  
33 such evaluation involved a controlled or real-world study;

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

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

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

44 (vi) Whether the police agency, police officer or peace officer  
45 considered a less-intrusive alternative prior to utilizing the technolo-  
46 gy, and if so, a description of such an explanation for why such alter-  
47 native was not ultimately used; and

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

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

54 (i) Acquire, access, or use any biometric recognition technology or  
55 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;



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

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

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

11    (vi) The risk of an unauthorized access to or breach of retained biom-  
12    etric data, safeguards or security measures designed to mitigate any  
13    such risk, and appropriate consequences for failure to adhere to such  
14    safeguards or security measures in the event of unauthorized access or a  
15    breach; and

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

22    (b) Transmit an equity impact assessment as defined in subdivision one  
23    of this section to the governor, the temporary president of the senate,  
24    the speaker of the assembly, the minority leader of the senate, and the  
25    minority leader of the assembly as well as publishing such assessment to  
26    the state agency, police agency, or the state police's own web page.

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

32    § 4. This act shall take effect immediately.