

SENATE No. 3084

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Second General Court
(2021-2022)

SENATE, July 30, 2022.

The committee on Senate Ways and Means, to whom was referred the House Bill to improve and modernize the information technology systems and capacities of the judiciary (House, No. 5076),- reported, in part (in so much as relates to section 63), a "Bill to regulate face surveillance" (Senate, No. 3084).

For the committee,
Michael J. Rodrigues

SENATE No. 3084

The Commonwealth of Massachusetts

**In the One Hundred and Ninety-Second General Court
(2021-2022)**

An Act to regulate face surveillance.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

1 Chapter 6 of the General Laws, as amended by chapter 253 of the acts of 2020, is hereby
2 amended by striking section 220 and inserting in place thereof the following section: -

3 Section 220. (a) As used in this section, the following words shall, unless the context
4 clearly requires otherwise, have the following meanings:

5 “Biometric surveillance technology”, any computer software that performs facial
6 recognition or other remote biometric recognition.

7 “Facial recognition”, an automated or semi-automated process that assists in identifying
8 or verifying an individual or analyzing or capturing information about an individual based on the
9 physical characteristics of an individual’s face, head or body, or that uses characteristics of an
10 individual’s face, head or body to derive information about the associations, activities or location
11 of an individual; provided, however, that “facial recognition” shall not include the use of search
12 terms to sort images in a database.

13 “Facial recognition search”, the use of facial recognition to analyze an image.

14 “Law enforcement agency”, as defined in section 1 of chapter 6E.

15 “Law enforcement officer” or “officer”, as defined in section 1 of chapter 6E.

16 “Other remote biometric recognition”, an automated or semi-automated process that
17 assists in identifying or verifying an individual or analyzing or capturing information about an
18 individual based on an individual’s gait, voice or other biometric characteristic or that uses such
19 characteristics to derive information about the associations, activities or location of an
20 individual; provided, however, that “other remote biometric recognition” shall not include the
21 identification or verification of an individual using deoxyribonucleic acid, fingerprints, palm
22 prints or other information derived from physical contact.

23 “Public agency”, any: (i) agency, executive office, department, board, commission,
24 bureau, division or authority of the commonwealth; (ii) political subdivision thereof; or (iii)
25 authority established by the general court to serve a public purpose.

26 “Public official”, any officer, employee, agent, contractor or subcontractor of any public
27 agency.

28 (b) Absent express authorization in a general or special law to the contrary, it shall be
29 unlawful for a law enforcement agency or officer to acquire, possess, access, use, assist with the
30 use of or provide resources for the development or use of any biometric surveillance technology,
31 or to enter into a contract with or make a request to a third party, including any federal agency,
32 for the purpose of acquiring, possessing, accessing or using information derived from a biometric
33 surveillance technology.

34 Except in a judicial proceeding alleging a violation of this section, no information
35 obtained in violation of this section shall be admissible in any criminal, civil, administrative or
36 other proceeding.

37 (c) The registrar of motor vehicles may acquire, possess, or use facial recognition
38 technology to verify an individual's identity when issuing licenses, permits or other documents
39 pursuant to chapter 90; provided, however, that the registrar shall not allow any other entity to
40 access or otherwise use its facial recognition technology except in accordance with subsection
41 (d).

42 (d) The department of state police may perform a facial recognition search, or request the
43 federal bureau of investigation to perform such a search, for the following purposes:

44 (1) to execute a warrant duly authorized by a judge based on probable cause that an
45 unidentified or unconfirmed individual in an image has committed a felony;

46 (2) upon reasonable belief that an emergency involving immediate danger of death or
47 serious physical injury to any individual or group of people requires the performance of a facial
48 recognition search without delay;

49 (3) to identify a deceased person; or

50 (4) on behalf of another law enforcement agency or a federal agency, provided that
51 such agency obtained a warrant pursuant to clause (1) or documented in writing the reason for a
52 search requested under clauses (2) or (3).

53 One facial recognition operations group within the department shall be charged with
54 receiving and evaluating law enforcement requests for facial recognition searches, performing

55 facial recognition searches, reporting results, and recording relevant data. The department shall
56 only use existing facial recognition technology used by the registrar of motor vehicles or federal
57 bureau of investigations or facial recognition technology approved by the executive office of
58 technology services and security, which may only be approved following a public hearing on the
59 proposed software.

60 Any search performed or search request made to the federal bureau of investigation under
61 this section shall be documented in writing.

62 (e) For any emergency facial recognition search performed or requested under subsection
63 (d)(2), the law enforcement agency shall immediately document the factual basis for its belief
64 that an emergency requires the performance of such a search without delay, and any emergency
65 facial recognition search shall be narrowly tailored to address the emergency. Not later than 48
66 hours after the law enforcement agency obtains access to the results of a facial recognition
67 search, the agency shall file with the superior court in the relevant jurisdiction a signed, sworn
68 statement made by a supervisory official of a rank designated by the head of the agency setting
69 forth the grounds for the emergency search.

70 (f) All individuals charged with a crime who were identified using a facial recognition
71 search under this subsection shall be provided notice that they were subject to such search,
72 pursuant to rule 14 of the rules of criminal procedure. Law enforcement agencies and district
73 attorneys must make readily available to defendants and their attorneys in criminal prosecutions
74 all records and information pertaining to any facial recognition searches performed or requested
75 during the course of the investigation of the crime or offense that is the object of the criminal
76 prosecution. This information shall include, but not be limited to, the results of the facial

77 recognition search (including other possible matches identified by the search), as well as records
78 regarding the particular program or algorithm used to conduct the facial recognition search, the
79 accuracy rate of the facial recognition system, any audit testing of the facial recognition system,
80 the identity of the individual or individuals who conducted the facial recognition search, training
81 provided to law enforcement officials involved in conducting facial recognition searches, and the
82 process by which the defendant was selected as the most likely match.

83 (g) The department shall document, as a public record, each facial recognition search
84 request and each facial recognition search performed pursuant to this section and report this
85 information quarterly to the executive office of public safety and security. Reported information
86 shall include: the date and time of the search or request; the system used for the search; the
87 specific criminal offense or offenses under investigation; the number of matched individuals
88 returned, if any; the name and position of the requesting individual and employing law
89 enforcement agency; a copy of the warrant or, if no warrant exists, a copy of the written
90 emergency request; and data detailing the individual characteristics included in the facial
91 recognition search or request, including the presumed race and gender of the person in the probe
92 image(s), as assessed by the officer conducting the search.

93 (h) Annually, not later than March 31, the executive office of public safety and security
94 shall publish on its website the following data for the previous calendar year: (i) the total number
95 of facial recognition searches performed by the department of state police, disaggregated by law
96 enforcement agency or federal agency on whose behalf the search was performed; (ii) the total
97 number of facial recognition searches performed by the federal bureau of investigation on behalf
98 of law enforcement agencies, disaggregated by law enforcement agency on whose behalf the
99 search was performed. For each category of data and each law enforcement agency, the

100 published information shall include: the number of searches performed pursuant to a warrant, by
101 alleged offense; the number of searches performed pursuant to an emergency; and the race and
102 gender of the subjects of the searches, as assessed by the officer conducting the search.

103 (i) Each non-law enforcement public agency shall document, as a public record, each
104 facial recognition search requested and each facial recognition search performed by its public
105 officials and report this information quarterly to the executive office of public safety and
106 security. Reported information shall include: the date and time of the search or request; the name
107 and position of the requesting individual; the reason for the search or request; the name, position,
108 and employer of the individual who conducted the search; the system used for the search; the
109 number of matched individuals returned, if any; and data detailing the individual characteristics
110 included in the facial recognition search or request, including the presumed race and gender of
111 the person in the probe image(s), as assessed by the individual conducting the search.

112 (j) Annually, not later than March 31, the executive office of public safety and security
113 shall publish on its website the following data for the previous calendar year: (i) the total number
114 of facial recognition searches performed by or at the request of non-law enforcement public
115 agencies, disaggregated by the public agency on whose behalf the search was performed. For
116 each public agency, the published information shall include the race and gender of the subjects of
117 the searches, as assessed by the individual conducting the search.

118 (k) Notwithstanding subsection (b), it shall be unlawful for a law enforcement agency of
119 officer to use a biometric surveillance system to infer a person's emotions or affect. It shall also
120 be unlawful for a law enforcement agency or officer to use a biometric surveillance system to
121 analyze moving images or video data, whether in real time or as applied to archived information;

122 provided, however, that facial recognition may be used on a still image taken from moving
123 images or video data if authorized pursuant to subsection (d).

124 (l) Notwithstanding subsection (b), a law enforcement agency or officer may: (i) acquire
125 and possess personal electronic devices, such as a cell phone or tablet, that utilize facial
126 recognition technology for the sole purpose of user authentication; (ii) acquire, possess and use
127 automated video or image redaction software; provided, that such software does not have the
128 capability of performing facial recognition or other remote biometric recognition; and (iii)
129 receive evidence related to the investigation of a crime derived from a biometric surveillance
130 technology; provided, that the use of a biometric surveillance technology was not knowingly
131 solicited by a law enforcement agency or officer in violation of subsection (b).