

**SENATE . . . . . No. 47**

**The Commonwealth of Massachusetts**

PRESENTED BY:

***Cynthia Stone Creem***

*To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:*

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

**An Act to regulate face surveillance.**

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
<i>Cynthia Stone Creem</i>	<i>First Middlesex and Norfolk</i>	
<i>Joanne M. Comerford</i>	<i>Hampshire, Franklin and Worcester</i>	<i>2/22/2021</i>
<i>Jason M. Lewis</i>	<i>Fifth Middlesex</i>	<i>2/23/2021</i>
<i>Jack Patrick Lewis</i>	<i>7th Middlesex</i>	<i>2/23/2021</i>
<i>Carmine Lawrence Gentile</i>	<i>13th Middlesex</i>	<i>2/23/2021</i>
<i>Rebecca L. Rausch</i>	<i>Norfolk, Bristol and Middlesex</i>	<i>2/24/2021</i>
<i>Maria Duaine Robinson</i>	<i>6th Middlesex</i>	<i>2/24/2021</i>
<i>Michael J. Barrett</i>	<i>Third Middlesex</i>	<i>3/2/2021</i>
<i>Erika Uyterhoeven</i>	<i>27th Middlesex</i>	<i>3/2/2021</i>
<i>Joseph A. Boncore</i>	<i>First Suffolk and Middlesex</i>	<i>3/4/2021</i>
<i>Julian Cyr</i>	<i>Cape and Islands</i>	<i>3/24/2021</i>
<i>Sal N. DiDomenico</i>	<i>Middlesex and Suffolk</i>	<i>4/1/2021</i>
<i>Patrick M. O'Connor</i>	<i>Plymouth and Norfolk</i>	<i>4/14/2021</i>
<i>Sonia Chang-Diaz</i>	<i>Second Suffolk</i>	<i>9/21/2021</i>
<i>Adam J. Scanlon</i>	<i>14th Bristol</i>	<i>11/30/2021</i>

**SENATE . . . . . No. 47**

---

---

By Ms. Creem, a petition (accompanied by bill, Senate, No. 47) of Cynthia Stone Creem, Joanne M. Comerford, Jason M. Lewis, Jack Patrick Lewis and other members of the General Court for legislation to regulate face surveillance. Advanced Information Technology, the Internet and Cybersecurity.

---

---

**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           SECTION 1. Chapter 6 of the General Laws, as amended by Chapter 253 of the Acts of  
2   2020, is hereby amended by striking Section 220 and inserting in place thereof the following new  
3   section:-

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

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

8           “Facial recognition”, an automated or semi-automated process that assists in identifying  
9   or verifying an individual or capturing information about an individual based on the physical  
10   characteristics of an individual’s face, head or body, or that uses characteristics of an individual’s  
11   face, head or body to infer emotion, associations, activities or the location of an individual;

12 provided, however, that “facial recognition” shall not include the use of search terms to sort  
13 images in a database.

14 “Facial recognition search”, a computer search using facial recognition to attempt to  
15 identify an unidentified person by comparing an image containing the face of the unidentified  
16 person to a set of images of identified persons; provided, however, that a set of images shall not  
17 include moving images or video data.

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

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

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

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

31 (b) Absent express authorization in a general or special law to the contrary, it shall be  
32 unlawful for a public agency or public official to acquire, possess, access, use, assist with the use

33 of or provide resources for the development or use of any biometric surveillance system, or to  
34 enter into a contract with or make a request to any third party, including any federal agency, for  
35 the purpose of acquiring, possessing, accessing or using information derived from a biometric  
36 surveillance system.

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

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

45 (d) The department of state police may perform a facial recognition search, or request the  
46 Federal Bureau of Investigation to perform such a search, for the following purposes:

47 (1) to execute a warrant duly authorized by a justice of the superior court based on  
48 probable cause that the search will to lead to evidence of the commission of a violent felony  
49 offense under the laws of the commonwealth;

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

53 (3) to identify a deceased person; or

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

57 To perform a facial recognition search, the department shall only use facial recognition  
58 technology acquired by the registrar of motor vehicles to search images in the registry of motor  
59 vehicles identification database.

60 Any search performed or search request made to the Federal Bureau of Investigation  
61 under 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 the 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 identified using a facial recognition search under this subsection shall  
71 be provided notice that they were subject to such search within 7 days after the law enforcement  
72 agency receives records or other information resulting from it. The law enforcement agency may  
73 apply for an order for delayed notice. Such order shall be issued by (i) the court that issued the  
74 order authorizing the facial recognition search, or (ii) in the case of an emergency search, the  
75 court where the sworn statement setting forth the grounds for such emergency search was filed.

76 Any order for delayed notice shall detail to the fullest extent possible, without  
77 endangering the public, the reasons why providing notice to the person subjected to the facial  
78 recognition search would constitute an immediate threat to public safety, and shall not be valid  
79 for more than 7 days without a further order for delayed notice.

80 (g) Law enforcement agencies and district attorneys must make readily available to  
81 defendants and their attorneys in criminal prosecutions all records and information pertaining to  
82 any facial recognition searches performed or requested during the course of the investigation of  
83 the crime or offense that is the object of the criminal prosecution. This information shall include,  
84 but not be limited to, the results of the facial recognition search (including other possible  
85 matches identified by the search), as well as records regarding the particular program or  
86 algorithm used to conduct the facial recognition search, the accuracy rate of the facial  
87 recognition system, any audit testing of the facial recognition system, the identity of the  
88 individual or individuals who conducted the facial recognition search, training provided to law  
89 enforcement officials involved in conducting facial recognition searches, and the process by  
90 which the defendant was selected as the most likely match.

91 (h) The executive office of public safety and security shall document, as a public record,  
92 each facial recognition search performed by the department of state police, each law enforcement  
93 agency or federal agency request for a facial recognition search made to the department of state  
94 police, and each department of state police request for a facial recognition search made to the  
95 Federal Bureau of Investigation. Such documentation shall include: the date and time of the  
96 search or request; the race and gender of the subject of the search or request; the number of  
97 matches returned, if any; the name and position of the requesting individual and employing law  
98 enforcement agency; a copy of the warrant, or in the case of an emergency, a copy of the written

99 emergency request; and data detailing any individual characteristics included in the facial  
100 recognition search or request.

101 (i) Annually, not later than March 31, the executive office of public safety and security  
102 shall publish on its website the following data for the previous calendar year: (i) the total number  
103 of facial recognition searches performed by the department of state police, disaggregated by law  
104 enforcement agency or federal agency on whose behalf the search was performed; (ii) the total  
105 number of facial recognition searches performed by the Federal Bureau of Investigation on  
106 behalf of law enforcement agencies, disaggregated by law enforcement agency on whose behalf  
107 the search was performed. For each category of data and each law enforcement agency, the  
108 published information shall include: the number of searches performed pursuant to a warrant, by  
109 alleged offense; the number of searches performed pursuant to an emergency; and the race and  
110 gender of the subjects of the searches.

111 (j) Notwithstanding subsection (b), a public agency may: (i) acquire and possess personal  
112 electronic devices, such as a cell phone or tablet, that utilizes facial recognition technology for  
113 the sole purpose of user authentication; (ii) acquire, possess and use automated video or image  
114 redaction software; provided, that such software does not have the capability of performing facial  
115 recognition or other remote biometric recognition; and (iii) receive evidence related to the  
116 investigation of a crime derived from a biometric surveillance system; provided, that the use of a  
117 biometric surveillance system was not knowingly solicited by a public agency or any public  
118 official in violation of subsection (b).