SENATE DOCKET, NO. 2134 FILED ON: 2/19/2021

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

SENATE DOCKET, NO. 2134 FILED ON: 2/19/2021

# 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:*

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

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

"Biometric surveillance system", any computer software that performs facial recognition or other remote biometric recognition.

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

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

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

"Law enforcement agency", as defined in section 1 of chapter 6E.

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

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

"Public official", any officer, employee, agent, contractor or subcontractor of any public agency.

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

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

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

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

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

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

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

(3) to identify a deceased person; or

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

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

Any search performed or search request made to the Federal Bureau of Investigation under this section shall be documented in writing.

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

(f) All individuals identified using a facial recognition search under this subsection shall be provided notice that they were subject to such search within 7 days after the law enforcement agency receives records or other information resulting from it. The law enforcement agency may apply for an order for delayed notice. Such order shall be issued by (i) the court that issued the order authorizing the facial recognition search, or (ii) in the case of an emergency search, the court where the sworn statement setting forth the grounds for such emergency search was filed.

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

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

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

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

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

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