

STATE OF MAINE

—
IN THE YEAR OF OUR LORD
TWO THOUSAND TWENTY-ONE

—
H.P. 1174 - L.D. 1585

An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials

Be it enacted by the People of the State of Maine as follows:

Sec. 1. 25 MRSA Pt. 14 is enacted to read:

PART 14

SURVEILLANCE

CHAPTER 701

FACIAL SURVEILLANCE

§6001. Facial surveillance

1. Definitions. As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

A. "Another jurisdiction" has the same meaning as in Title 17-A, section 2, subsection 3-B.

B. "Bureau of Motor Vehicles" means the Department of the Secretary of State, Bureau of Motor Vehicles.

C. "Department" means a state, county or municipal government or a department, agency or subdivision thereof or any other entity identified in law as a public instrumentality, including, but not limited to, a law enforcement agency.

D. "Facial surveillance" means an automated or semi-automated process that assists in identifying or verifying an individual, or in capturing information about an individual, based on the physical characteristics of an individual's face.

E. "Facial surveillance system" means any computer software or application that performs facial surveillance.

F. "Law enforcement agency" has the same meaning as in section 3701, subsection 1.

G. "Public employee" means a person employed by a department, including, but not limited to, a law enforcement officer.

H. "Public official" means a person elected or appointed to a public office that is part of a department.

I. "Serious crime" means:

(1) A crime under the laws of this State that:

(a) Is punishable by a term of imprisonment of one year or more; or

(b) Is a Class D or Class E crime under the laws of this State that is a violation of Title 17-A, chapter 9, 11, 12, 13 or 35; Title 15, section 1092, if the violation is based on a condition under Title 15, section 1026, subsection 3, paragraph A, subparagraph (5) or (8); or Title 19-A, section 4011; or

(2) A crime under the laws of another jurisdiction that:

(a) Has, as an element, the use of a firearm or other dangerous weapon against a person;

(b) Is elementally substantially similar to a crime under subparagraph (1); or

(c) Is punishable by a term of imprisonment of one year or more.

2. Use of facial surveillance by department, public employee or public official.

The following provisions govern the use of facial surveillance systems and facial surveillance data by a department or by a public employee or public official in the performance of their official duties.

A. Except as provided in paragraphs B and D, a department, public employee or public official may not:

(1) Obtain, retain, possess, access, request or use a facial surveillance system or information derived from a search of a facial surveillance system;

(2) Enter into an agreement with a 3rd party for the purpose of obtaining, retaining, possessing, accessing or using, by or on behalf of a department, public employee or public official, a facial surveillance system or information derived from a search of a facial surveillance system; or

(3) Issue a permit or enter into any other agreement that authorizes a 3rd party to obtain, retain, possess, access or use a facial surveillance system or information derived from a search of a facial surveillance system.

B. Notwithstanding the provisions of paragraph A, a department, public employee or public official may request a search of a facial surveillance system as provided in paragraph C and may obtain, retain, possess, access or use the results of a search of a facial surveillance system, as provided in paragraph C, for the purposes of:

(1) Investigating a serious crime, when there is probable cause to believe that an unidentified individual in an image has committed the serious crime;

(2) Assisting in the identification of a person who is deceased or believed to be deceased;

- (3) Assisting in the identification of a missing or endangered person; or
- (4) Performing a duty authorized under paragraph D, subparagraph (1), if the Bureau of Motor Vehicles or a public employee or public official of the Bureau of Motor Vehicles makes the request for the search of the facial surveillance system.

C. The following provisions apply when a department, public employee or public official requests a search of a facial surveillance system under paragraph B, subparagraph (1), (2) or (3).

(1) A request for a search of the facial surveillance system within the State must be made to the Bureau of Motor Vehicles.

(2) Except as provided in subparagraph (3), a request for a search of the facial surveillance system of a state agency that issues government credentials in another jurisdiction or the Federal Bureau of Investigation must be made to the State Police unless there is an emergency posing an imminent danger of death or serious physical injury. If an emergency exists under this subparagraph, the department, public employee or public official may request the search directly from a state agency that issues government credentials in another jurisdiction or the Federal Bureau of Investigation and shall file a report of the request with the State Police as soon as practicable.

(3) The Bureau of Motor Vehicles may request a search of a facial surveillance system from a state agency that issues government credentials in another jurisdiction or the Federal Bureau of Investigation for the purposes of fraud prevention or investigation.

D. Nothing in paragraph A prohibits a department, public employee or public official from:

(1) Obtaining, maintaining or using a facial surveillance system or the results of a search of a facial surveillance system within the Bureau of Motor Vehicles in accordance with Title 29-A, section 1401, subsection 9 or for the purposes of fraud prevention or investigation;

(2) Using facial surveillance technology that analyzes the eye's iris in a regional jail or county jail;

(3) Using evidence that has been generated from a search of a facial surveillance system that is related to an investigation of a specific crime;

(4) Obtaining or possessing for evidentiary purposes an electronic device, including, but not limited to, a cellular telephone, tablet or computer, that performs facial surveillance for the sole purpose of user authentication;

(5) Using social media or communications software or applications for communicating with the public as long as such use does not include the affirmative use of facial surveillance;

(6) Using automated redaction software as long as such software is not capable of performing facial surveillance;

(7) Performing duties required by the National Child Search Assistance Act of 1990, 34 United States Code, Sections 41307 and 41308 (2021); or

(8) Using facial surveillance on an electronic device, including, but not limited to, a cellular telephone, tablet or computer, owned by the public employee or public official for that person's personal use for the sole purpose of user authentication of that person.

E. Facial surveillance data does not, without other evidence, establish probable cause justifying arrest, search or seizure.

F. The State Police and the Bureau of Motor Vehicles shall maintain logs that track all requests for searches of facial surveillance systems received and performed pursuant to paragraph C. De-identified logs containing the date of the search request, the name of the public employee or public official who made the request and the name of the department for which the employee or official works, the databases searched, the statutory offense under investigation and the race and sex of the person under investigation are public records for the purpose of Title 1, chapter 13, subchapter 1. The provisions of Title 16, chapter 9 do not apply to records created or maintained pursuant to this paragraph.

3. Enforcement. The following provisions apply to a violation of this section by a department or a public employee or public official acting in the performance of their official duties.

A. Facial surveillance data collected or derived in violation of this section:

(1) Must be considered unlawfully obtained and, except as otherwise provided by law, must be deleted upon discovery; and

(2) Is inadmissible in evidence in any proceeding in or before any public official, department, regulatory body or authority.

B. A person injured or aggrieved by a violation of this section may bring an action in a court in this State against the department, public employee or public official having possession, custody or control of facial surveillance data in violation of this section and may seek injunctive or declaratory relief or a writ of mandamus.

C. A public employee or public official who, in the performance of their official duties, violates this section may be subject to disciplinary action, including, but not limited to, retraining, suspension or termination, subject to the requirements of due process and of any applicable collective bargaining agreement.

D. Nothing in this subsection limits the rights under state or federal law of a person injured or aggrieved by a violation of this section.

Sec. 2. Effective date. This Act takes effect October 1, 2021.