Assembly Bill No. 1215

CHAPTER 579

An act to add and repeal Section 832.19 of the Penal Code, relating to law enforcement.

[Approved by Governor October 8, 2019. Filed with Secretary of State October 8, 2019.]

LEGISLATIVE COUNSEL'S DIGEST

AB 1215, Ting. Law enforcement: facial recognition and other biometric surveillance.

Existing law states the intent of the Legislature to establish policies and procedures to address issues related to the downloading and storage of data recorded by a body-worn camera worn by a peace officer, and requires that those policies and procedures be based on best practices. Existing law requires law enforcement agencies, departments, or entities to consider certain best practices regarding the downloading and storage of body-worn camera data when establishing policies and procedures for the implementation and operation of a body-worn camera system, as specified.

This bill would prohibit a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera. The bill would authorize a person to bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition.

The bill would repeal these provisions on January 1, 2023.

The people of the State of California do enact as follows:

SECTION 1. The Legislature finds and declares all of the following:

(a) Californians value privacy as an essential element of their individual freedom, and are guaranteed a right to privacy in Section 1 of Article I of the California Constitution.

(b) Facial recognition and other biometric surveillance technology pose unique and significant threats to the civil rights and civil liberties of residents and visitors.

(c) The use of facial recognition and other biometric surveillance is the functional equivalent of requiring every person to show a personal photo identification card at all times in violation of recognized constitutional rights. This technology also allows people to be tracked without consent. It would also generate massive databases about law-abiding Californians, and may chill the exercise of free speech in public places.

(d) Facial recognition and other biometric surveillance technology has been repeatedly demonstrated to misidentify women, young people, and people of color and to create an elevated risk of harmful "false positive" identifications.

(e) Facial and other biometric surveillance would corrupt the core purpose of officer-worn body-worn cameras by transforming those devices from transparency and accountability tools into roving surveillance systems.

(f) The use of facial recognition and other biometric surveillance would disproportionately impact the civil rights and civil liberties of persons who live in highly policed communities. Its use would also diminish effective policing and public safety by discouraging people in these communities, including victims of crime, undocumented persons, people with unpaid fines and fees, and those with prior criminal history from seeking police assistance or from assisting the police.

SEC. 2. Section 832.19 is added to the Penal Code, immediately following Section 832.18, to read:

832.19. (a) For the purposes of this section, the following terms have the following meanings:

(1) "Biometric data" means a physiological, biological, or behavioral characteristic that can be used, singly or in combination with each other or with other information, to establish individual identity.

(2) "Biometric surveillance system" means any computer software or application that performs facial recognition or other biometric surveillance.

(3) "Facial recognition or other biometric surveillance" means either of the following, alone or in combination:

(A) An automated or semiautomated process that captures or analyzes biometric data of an individual to identify or assist in identifying an individual.

(B) An automated or semiautomated process that generates, or assists in generating, surveillance information about an individual based on biometric data.

(4) "Facial recognition or other biometric surveillance" does not include the use of an automated or semiautomated process for the purpose of redacting a recording for release or disclosure outside the law enforcement agency to protect the privacy of a subject depicted in the recording, if the process does not generate or result in the retention of any biometric data or surveillance information.

(5) "Law enforcement agency" means any police department, sheriff's department, district attorney, county probation department, transit agency police department, school district police department, highway patrol, the police department of any campus of the University of California, the California State University, or a community college, the Department of the California Highway Patrol, and the Department of Justice.

(6) "Law enforcement officer" means an officer, deputy, employee, or agent of a law enforcement agency.

(7) "Officer camera" means a body-worn camera or similar device that records or transmits images or sound and is attached to the body or clothing of, or carried by, a law enforcement officer.

(8) "Surveillance information" means either of the following, alone or in combination:

(A) Any information about a known or unknown individual, including, but not limited to, a person's name, date of birth, gender, or criminal background.

(B) Any information derived from biometric data, including, but not limited to, assessments about an individual's sentiment, state of mind, or level of dangerousness.

(9) "Use" means either of the following, alone or in combination:

(A) The direct use of a biometric surveillance system by a law enforcement officer or law enforcement agency.

(B) A request or agreement by a law enforcement officer or law enforcement agency that another law enforcement agency or other third party use a biometric surveillance system on behalf of the requesting officer or agency.

(b) A law enforcement agency or law enforcement officer shall not install, activate, or use any biometric surveillance system in connection with an officer camera or data collected by an officer camera.

(c) In addition to any other sanctions, penalties, or remedies provided by law, a person may bring an action for equitable or declaratory relief in a court of competent jurisdiction against a law enforcement agency or law enforcement officer that violates this section.

(d) This section does not preclude a law enforcement agency or law enforcement officer from using a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification if this use is lawful and does not generate or result in the retention of any biometric data or surveillance information.

(e) This section shall remain in effect only until January 1, 2023, and as of that date is repealed.

O