Assembly Bill No. 69

CHAPTER 461

An act to add Section 832.18 to the Penal Code, relating to peace officers.

[Approved by Governor October 3, 2015. Filed with Secretary of State October 3, 2015.]

LEGISLATIVE COUNSEL'S DIGEST

AB 69, Rodriguez. Peace officers: body-worn cameras.

Existing law makes it a crime to intentionally record a confidential communication without the consent of all parties to the communication. Existing law exempts specified peace officers from that provision if they are acting within the scope of their authority.

This bill would require law enforcement agencies to consider specified best practices when establishing policies and procedures for downloading and storing data from body-worn cameras, including, among other things, prohibiting the unauthorized use, duplication, or distribution of the data, and establishing storage periods for evidentiary and nonevidentiary data, as defined.

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

SECTION 1. Section 832.18 is added to the Penal Code, to read:

832.18. (a) It is the intent of the Legislature to establish policies and procedures to address issues related to the downloading and storage data recorded by a body-worn camera worn by a peace officer. These policies and procedures shall be based on best practices.

(b) When establishing policies and procedures for the implementation and operation of a body-worn camera system, law enforcement agencies, departments, or entities shall consider the following best practices regarding the downloading and storage of body-worn camera data:

(1) Designate the person responsible for downloading the recorded data from the body-worn camera. If the storage system does not have automatic downloading capability, the officer's supervisor should take immediate physical custody of the camera and should be responsible for downloading the data in the case of an incident involving the use of force by an officer, an officer-involved shooting, or other serious incident.

(2) Establish when data should be downloaded to ensure the data is entered into the system in a timely manner, the cameras are properly maintained and ready for the next use, and for purposes of tagging and categorizing the data.

(3) Establish specific measures to prevent data tampering, deleting, and copying, including prohibiting the unauthorized use, duplication, or distribution of body-worn camera data.

(4) Categorize and tag body-worn camera video at the time the data is downloaded and classified according to the type of event or incident captured in the data.

(5) Specifically state the length of time that recorded data is to be stored.

(A) Unless subparagraph (B) or (C) applies, nonevidentiary data including video and audio recorded by a body-worn camera should be retained for a minimum of 60 days, after which it may be erased, destroyed, or recycled. An agency may keep data for more than 60 days to have it available in case of a citizen complaint and to preserve transparency.

(B) Evidentiary data including video and audio recorded by a body-worn camera under this section should be retained for a minimum of two years under any of the following circumstances:

(i) The recording is of an incident involving the use of force by a peace officer or an officer-involved shooting.

(ii) The recording is of an incident that leads to the detention or arrest of an individual.

(iii) The recording is relevant to a formal or informal complaint against a law enforcement officer or a law enforcement agency.

(C) If evidence that may be relevant to a criminal prosecution is obtained from a recording made by a body-worn camera under this section, the law enforcement agency should retain the recording for any time in addition to that specified in paragraphs (A) and (B), and in the same manner as is required by law for other evidence that may be relevant to a criminal prosecution.

(D) In determining a retention schedule, the agency should work with its legal counsel to determine a retention schedule to ensure that storage policies and practices are in compliance with all relevant laws and adequately preserve evidentiary chains of custody.

(E) Records or logs of access and deletion of data from body-worn cameras should be retained permanently.

(6) State where the body-worn camera data will be stored, including, for example, an in-house server which is managed internally, or an online cloud database which is managed by a third-party vendor.

(7) If using a third-party vendor to manage the data storage system, the following factors should be considered to protect the security and integrity of the data:

(A) Using an experienced and reputable third-party vendor.

(B) Entering into contracts that govern the vendor relationship and protect the agency’s data.

(C) Using a system that has a built-in audit trail to prevent data tampering and unauthorized access.

(D) Using a system that has a reliable method for automatically backing up data for storage.

(E) Consulting with internal legal counsel to ensure the method of data storage meets legal requirements for chain-of-custody concerns.

(F) Using a system that includes technical assistance capabilities.

(8) Require that all recorded data from body-worn cameras are property of their respective law enforcement agency and shall not be accessed or released for any unauthorized purpose, explicitly prohibit agency personnel from accessing recorded data for personal use and from uploading recorded data onto public and social media Internet Web sites, and include sanctions for violations of this prohibition.

(c) (1) For purposes of this section, "evidentiary data" refers to data of an incident or encounter that could prove useful for investigative purposes, including, but not limited to, a crime, an arrest or citation, a search, a use of force incident, or a confrontational encounter with a member of the public. The retention period for evidentiary data are subject to state evidentiary laws.

(2) For purposes of this section, "nonevidentiary data" refers to data that does not necessarily have value to aid in an investigation or prosecution, such as data of an incident or encounter that does not lead to an arrest or citation, or data of general activities the officer might perform while on duty.

(d) Nothing in this section shall be interpreted to limit the public's right to access recorded data under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code).

O