

AMENDED IN ASSEMBLY APRIL 21, 2015
AMENDED IN ASSEMBLY MARCH 16, 2015
CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL

No. 69

Introduced by Assembly Member Rodriguez
(Coauthor: Assembly Member Weber)

December 18, 2014

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

LEGISLATIVE COUNSEL'S DIGEST

AB 69, as amended, 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 follow specified best practices when establishing policies and procedures for downloading and storing data from body-worn cameras, *including, among other things, prohibiting unauthorized use, duplication, or distribution of the data, storage periods for evidentiary and nonevidentiary data, as defined.*

Vote: majority. Appropriation: no. Fiscal committee: no.
State-mandated local program: no.

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

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

3 832.18. (a) It is the intent of the Legislature to establish
4 policies and procedures to address issues related to the
5 downloading and storage data recorded by a body-worn camera
6 worn by a peace officer. These policies and procedures shall be
7 based on best practices.

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

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

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

24 (3) ~~Include~~—Establish specific measures to prevent data
25 tampering, deleting, and ~~copying~~ copying, *including prohibiting
26 the unauthorized use, duplication, or distribution of body-worn
27 camera data.*

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

31 (5) ~~State~~—Specifically state the length of time that recorded data
32 shall be stored.

33 (A) *Unless subparagraph (B) or (C) applies, a law enforcement
34 agency shall retain nonevidentiary data including video and audio
35 recorded by a body-worn camera for a minimum of one year, after
36 which it will be erased, destroyed, or recycled pursuant to Section
37 34090.6 of the Government Code.*

1 (B) A law enforcement agency shall retain evidentiary data
2 including video and audio recorded by a body-worn camera under
3 this section for a minimum of three years under any of the following
4 situations:

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

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

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

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

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

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

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

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

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

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

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

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

35 (c) (1) For purposes of this section, "evidentiary data" refers
36 to data of an incident or encounter that could prove useful for
37 investigative purposes, including, but not limited to, a crime, an
38 arrest or citation, a search, a use of force incident, or a
39 confrontational encounter with a member of the public. The

1 retention period for evidentiary data are subject to state evidentiary
2 laws.

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

8 (d) All recorded media, images, and audio from body-worn
9 cameras are property of their respective law enforcement agency,
10 and shall not be copied, released, or disseminated in any form or
11 manner outside the parameters of this section without the written
12 consent of the head of the agency, unless otherwise authorized by
13 law.