

AMENDED IN SENATE JULY 2, 2015  
AMENDED IN ASSEMBLY MAY 22, 2015  
AMENDED IN ASSEMBLY MAY 4, 2015  
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 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.

Vote: majority. Appropriation: no. Fiscal committee: yes.  
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 of  
18 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 are  
22 properly maintained and ready for the next use, and for purposes  
23 of tagging and categorizing the data.

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

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

30 (5) Specifically state the length of time that recorded data shall  
31 be stored.

32 (A) Unless subparagraph (B) or (C) applies, a law enforcement  
33 agency shall retain nonevidentiary data including video and audio  
34 recorded by a body-worn camera for a minimum of 60 days, after  
35 which it ~~will~~ *may* be erased, destroyed, or recycled. *An agency*

1 *may keep data for more than 60 days to have it available in case*  
2 *of a citizen complaint and to preserve transparency.*

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

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

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

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

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

19 (D) *An agency establishing procedures for a body-worn camera*  
20 *system shall work with its legal counsel to determine a retention*  
21 *schedule to ensure that storage policies and practices are in*  
22 *compliance with all relevant laws and adequately preserve*  
23 *evidentiary chains of custody.*

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

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

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

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

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

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

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

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

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

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

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

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

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