SENATE COMMITTEE ON PUBLIC SAFETY

Senator Loni Hancock, Chair
2015 - 2016 Regular

Bill No:	AB 69	**Hearing Date:**	July 14, 2015
Author:	Rodriguez		
Version:	July 2, 2015		
Urgency:	No	**Fiscal:**	Yes
Consultant:	JRD		

Subject: ***Peace Officers: Body-Worn Cameras***

HISTORY

Source: Author

Prior Legislation: None known

Support: California Public Defenders' Association

Opposition: None known

Assembly Floor Vote: 75 - 1

PURPOSE

The purpose of this legislation is to require law enforcement agencies to consider specified best practices when establishing policies and procedures for downloading and storing data from body-worn cameras.

Existing law defines "peace officer," as specified. (Penal Code § 830, et seq.)

Existing law makes it a crime for a person, intentionally and without requisite consent, to eavesdrop on a confidential communication by means of any electronic amplifying or recording device. (Penal Code § 632.)

Existing law exempts a number of law enforcement agencies from the prohibition in Penal Code section 632,[1] including the Attorney General, any district attorney, or any assistant, deputy, or investigator of the Attorney General or any district attorney, any officer of the California Highway Patrol, any chief of police, assistant chief of police, or police officer of a city or city and county, any sheriff, undersheriff, or deputy sheriff regularly employed and paid in that capacity by a county, police officer of the County of Los Angeles, or any person acting pursuant to the direction of one of these law enforcement officers acting within the scope of his or her authority. (Penal Code § 633.)

[1] Penal Code section 633 also exempts listed law enforcement from the prohibitions in sections 631, 632.5, 632.6, and 632.7.

This bill states 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.

This bill states that law enforcement agencies, departments, or entities must consider the following best practices when establishing policies and procedures for the implementation and operation of a body-worn camera system:

- 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.

- 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.

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

- 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;

- Specifically state the length of time that recorded data shall be stored;

    - Unless either of the paragraphs below applies, a law enforcement agency shall retain nonevidentiary data including video and audio recorded by a body-worn camera for a minimum of 60 days, after which it will be erased, destroyed, or recycled. Agencies may keep data longer to preserve transparency and to have it available in case a citizen complaint arises.

    - A law enforcement agency shall retain evidentiary data including video and audio recorded by a body-worn camera under this section for a minimum of two years when the recording is of an incident involving use of force or an officer-involved shooting, an incident that leads to the detention or arrest of an individual, or is relevant to a formal or informal complaint against an officer or a law enforcement agency.

    - If evidence that may be relevant to a criminal prosecution is obtained from a recording made by a body-worn camera, the law enforcement agency shall retain the recording for any time in addition to the amount of time specified above and in the same manner as is required by law for other evidence that may be relevant to a criminal prosecution.

    - Each agency must work with their 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 chain of custody.

    - Records or logs of access and deletion of data from body-worn cameras must be retained permanently.

- 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.

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

  - Using an experienced and reputable third-party vendor;

  - Entering into contracts that govern the vendor relationship and protect the agency's data;

  - Using a system that has a built in audit trail to prevent data tampering and unauthorized access;

  - Using a system that has a reliable method for automatically backing up data for storage;

  - Consulting with internal legal counsel to ensure the method of data storage meets legal requirements for chain-of-custody concerns; and

  - Using a system that includes technical assistance capabilities.

- 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.

*This bill d*efines "evidentiary data" as 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 is subject to state evidentiary laws.

*This bill d*efines "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.

This bill clarifies that the provisions in the bill shall not be interpreted to limit the public's right to access recorded data under the California Public Records Act.

RECEIVERSHIP/OVERCROWDING CRISIS AGGRAVATION

For the past eight years, this Committee has scrutinized legislation referred to its jurisdiction for any potential impact on prison overcrowding. Mindful of the United States Supreme Court ruling and federal court orders relating to the state's ability to provide a constitutional level of health care to its inmate population and the related issue of prison overcrowding, this Committee has applied its "ROCA" policy as a content-neutral, provisional measure necessary to ensure that the Legislature does not erode progress in reducing prison overcrowding.

On February 10, 2014, the federal court ordered California to reduce its in-state adult institution population to 137.5% of design capacity by February 28, 2016, as follows:

- 143% of design bed capacity by June 30, 2014;
- 141.5% of design bed capacity by February 28, 2015; and,
- 137.5% of design bed capacity by February 28, 2016.

In February of this year the administration reported that as "of February 11, 2015, 112,993 inmates were housed in the State's 34 adult institutions, which amounts to 136.6% of design bed capacity, and 8,828 inmates were housed in out-of-state facilities. This current population is now below the court-ordered reduction to 137.5% of design bed capacity." (Defendants' February 2015 Status Report In Response To February 10, 2014 Order, 2:90-cv-00520 KJM DAD PC, 3-Judge Court, *Coleman v. Brown, Plata v. Brown* (fn. omitted).

While significant gains have been made in reducing the prison population, the state now must stabilize these advances and demonstrate to the federal court that California has in place the "durable solution" to prison overcrowding "consistently demanded" by the court. (Opinion Re: Order Granting in Part and Denying in Part Defendants' Request For Extension of December 31, 2013 Deadline, NO. 2:90-cv-0520 LKK DAD (PC), 3-Judge Court, *Coleman v. Brown, Plata v. Brown* (2-10-14). The Committee's consideration of bills that may impact the prison population therefore will be informed by the following questions:

- Whether a proposal erodes a measure which has contributed to reducing the prison population;
- Whether a proposal addresses a major area of public safety or criminal activity for which there is no other reasonable, appropriate remedy;
- Whether a proposal addresses a crime which is directly dangerous to the physical safety of others for which there is no other reasonably appropriate sanction;
- Whether a proposal corrects a constitutional problem or legislative drafting error; and
- Whether a proposal proposes penalties which are proportionate, and cannot be achieved through any other reasonably appropriate remedy.

COMMENTS

1. Need for This Legislation

According to the author:

> While the 2012 Rialto Study on body-worn cameras concluded that there is a correlation between the use of body-worn cameras and the reduction of excessive use of force complaints, we must not lose sight that this is a developing technology and we have yet to learn and fully understand how this technology is being used in the field and the impact it has on police-citizen behavior and on crime. AB 69 focuses on providing guidelines for downloading and storing body-worn camera data for those law enforcement agencies that choose to implement a body-worn camera program.

2. Effect of This Legislation

A number of law enforcement agencies are currently permitted to utilize body-worn cameras. Existing law, however, does not require these agencies to have a policy prior to utilizing them. This legislation would require law enforcement to consider best practices for the retention of body-worn camera data should an agency draft a policy.

A recent report released by U.S. Department of Justice's Office of Community Oriented Policing Services and the Police Executive Research Forum studied the use of body-worn cameras by police agencies. (Miller and Toliver, *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned*, Police Executive Research Forum (Nov. 2014).) This research included a survey of 250 police agencies, interviews with more than 40 police executives, a review of 20 existing body-camera policies, and a national conference at which more than 200 police chiefs, sheriffs, federal justice representatives, and other experts shared their knowledge of and experiences with body-worn cameras. (*Id.*) The report shows that body-worn cameras can help agencies demonstrate transparency and address the community's questions about controversial events. (*Id.*) Among other reported benefits are that the presence of a body-worn camera have helped strengthen officer professionalism and helped to de-escalate contentious situations, and when questions do arise following an event or encounter, police having a video record helps lead to a quicker resolution. (*Id.*) The report made specified recommendations related to data storage and retention policies:

> **14. Policies should designate the officer as the person responsible for downloading recorded data from his or her body-worn camera. However, in certain clearly identified circumstances (e.g., officer-involved shootings, in-custody deaths, or other incidents involving the officer that result in a person's bodily harm or death), the officer's supervisor should immediately take physical custody of the camera and should be responsible for downloading the data.**
>
> **15. Policies should include specific measures to prevent data tampering, deleting, and copying.**
>
> Common strategies include the following:
>
> - Using data storage systems with built-in audit trails;
> - Requiring the supervisor to physically take custody of the officer's body-worn camera at the scene of a shooting or at another serious incident in which the officer was involved and to assume responsibility for downloading the data (see recommendation 14)
> - Conducting forensic reviews of the camera equipment when questions arise (e.g., if an officer claims that he or she failed to record an incident because the camera malfunctioned)
>
> **16. Data should be downloaded from the body-worn camera by the end of each shift in which the camera was used.**
>
> **Rationale**: First, many camera systems recharge and clear old data during the downloading process, so this policy helps to ensure cameras are properly maintained and ready for the next use. Second, events will be fresh in the

officer's memory for the purpose of tagging and categorizing. Third, this policy ensures evidence will be entered into the system in a timely manner.

17. Officers should properly categorize and tag body-worn camera videos at the time they are downloaded. Videos should be classified according to the type of event or incident captured in the footage.

If video contains footage that can be used in an investigation or captures a confrontational encounter between an officer and a member of the public, it should be deemed "evidentiary" and categorized and tagged according to the type of incident. If the video does not contain evidence or it captures a routine, non-confrontational encounter, it should be considered "non-evidentiary" or a "non-event."

Rationale: Proper labeling of recorded data is critical for two reasons. First, the retention time for recorded data typically depends on the category of the event captured in the video. Thus, proper tagging is critical for determining how long the data will be retained in the agency's system. Second, accurate tagging helps supervisors, prosecutors, and other authorized personnel to readily identify and access the data they need for investigations or court proceedings.

Lessons learned: Some agencies report that reviewing and tagging recorded data can be a time-consuming process that is prone to human error. One agency addressed this issue by working with the camera manufacturer to develop an automated process that links the recorded data to the agency's records management system. Some camera systems can also be linked to electronic tablets that officers can use to review and tag recorded data while still in the field.

18. Policies should specifically state the length of time that recorded data must be retained. For example, many agencies provide 60-day or 90-day retention times for non-evidentiary data.

Agencies should clearly state all retention times in the policy and make the retention times public by posting them on their websites to ensure community members are aware of the amount of time they have to request copies of video footage.

Retention times for recorded data are typically subject to state laws and regulations that govern other types of evidence. Agencies should consult with legal counsel to ensure retention policies are in compliance with these laws:

- For evidentiary data, most state laws provide specific retention times depending on the type of incident. Agencies should set retention times for recorded data to meet the minimum time required by law but may decide to keep recorded data longer.
- For non-evidentiary data, policies should follow state law requirements when applicable. However, if the law does not provide specific requirements for non-evidentiary data, the agency should set a retention time that takes into account the following:
    - Departmental policies governing retention of other types of electronic records

- Openness of the state's public disclosure laws
- Need to preserve footage to promote transparency and investigate citizen complaints
- Capacity for data storage

Agencies should obtain written approval for retention schedules from their legal counsel and prosecutors.

19. Policies should clearly state where body-worn camera videos are to be stored.

The decision of where to store recorded data will depend on each agency's needs and resources. PERF does not recommend any particular storage method. Agencies should consult with their department's legal counsel and with prosecutors to ensure the method for data storage meets any legal requirements and chain-of-custody needs.

Common storage locations include in-house servers (managed internally) and online cloud databases (managed by a third-party vendor).Some agencies burn recorded data to discs as part of the evidence file folder.

Lessons learned: Factors that agency leaders should consider when determining storage location include the following:

- Security concerns
- Reliable methods for backing up data
- Chain-of-custody issues
- Capacity for data storage

Lessons learned: Police executives and prosecutors report that they have had no issues to date with using a third-party vendor to manage recorded data on an online cloud, so long as the chain of custody can be properly established. When using a third-party vendor, the keys to protecting the security and integrity of the data include the following:

- Using a reputable, experienced third-party vendor
- Entering into a legal contract that governs the vendor relationship and protects the agency's data
- Using a system that has a built-in audit trail to prevent data tampering and unauthorized access
- Using a system that has a reliable method for automatically backing up data
- Consulting with prosecutors and legal advisors

(*Id*. at 42-45.)

This legislation seeks to help implement these recommendations by requiring law enforcement agencies to consider best practices regarding the downloading and storage of body-worn camera data.

3. Argument in Support

The California Public Defenders Association states:

> CPDA supports the use of body-worn cameras by law enforcement. Of equal importance to the wearing of body-worn cameras are policies concerning the use of these cameras and the proper storage of data collected from these cameras.
>
> CPDA believes that this bill is a good start in establishing these policies. Once the use of body-worn cameras by law enforcement becomes more common, these policies may need to be revisited and updated to ensure integrity in their use and integrity in the data captured by them.
>
> Further, CPDA believes that the use of body-worn cameras will help build trust between communities and their law enforcement officers, and promote the truth finding process.

-- END –