

HOUSE RESEARCH

Bill Summary

FILE NUMBER: S.F. 498

DATE: May 21, 2016

Version: Revised Conference Committee Report (CCRSF0498A)

Authors: Cornish

Subject: Portable Recording Systems (“Body Cameras”)

Analyst: Matt Gehring, 651-296-5052

This publication can be made available in alternative formats upon request. Please call 651-296-6753 (voice); or the Minnesota State Relay Service at 1-800-627-3529 (TTY) for assistance. Summaries are also available on our website at: www.house.mn/hrd/.

Overview

This bill establishes a data practices and regulatory system to govern the use of portable recording systems (commonly referred to as “body cameras”) by Minnesota law enforcement agencies.

Further specific details are provided in this summary, and in the text of the bill. In general, the following principles would apply:

- **Data Classifications:** “Non-incident” data and inactive criminal investigative data are private, with exceptions allowing public release if: (1) the data document an officer’s discharge of a firearm that requires a report to the BCA; (2) a peace officer uses force that results in substantial bodily harm; (3) if a data subject requests public release; or (4) if a court orders release. Active criminal investigative data is confidential, and other specific classifications provided in current law would continue to apply.
- **Retention:** In general, the data would be retained according to the law enforcement agency’s existing records retention schedule. “Non-incident” data must be retained for at least 90 days. Data that would become public under the classifications in this bill, and any data related to an incident where a complaint is filed against the officer, must be retained for at least one year. A data subject is permitted to request a longer retention period for possible evidentiary or exculpatory use of the data. Law enforcement is also permitted to retain investigative data beyond the retention schedule for possible evidentiary or exculpatory use.

Section

- **Peace officer access and redaction:** A peace officer is a data subject, and is permitted to access any recordings prior to completing the officer's written report on an incident. An on-duty peace officer may not be redacted from a video, unless the officer is working undercover.
- **Data security and audits:** A variety of data security standards and audit requirements are provided, based on current requirements of chapter 13. The agency would be required to arrange for biennial independent audits of its compliance with the law. In addition, enhanced civil penalties for willful violations of the law are added.
- **Portable recording system vendors:** Vendors who provide services to a law enforcement agency related to portable recording systems (such as hosting data storage in the cloud) must comply with all of the requirements of the Data Practices Act, and are subject to additional penalties for improper disclosure of data.
- **Written policies:** A law enforcement agency must adopt written policies governing use of a portable recording system. Members of the public must be permitted to provide comment on the policies in writing, and at a regularly-scheduled meeting of the jurisdiction's governing body.
- **Legislative auditor review:** A comprehensive review of compliance by the legislative auditor would be conducted in 2019.

Section

- 1 Arrest data.** Requires the public report created as a result of an arrest, citation, or incarceration to indicate whether the law enforcement agency used a portable recording system as part of that action.
- 2 Response or incident data.** Requires the public report created as a result of a law enforcement agency's response to a request for service to include whether the agency used a portable recording system as part of that response.
- 3 Criminal investigative data.** Adds video and audio records to the existing law that classifies inactive criminal investigative data as private or nonpublic, if the data are clearly offensive to common sensibilities.
- 4 Public benefit data.** Permits a law enforcement agency to release private or nonpublic public recording system data, if doing so would aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest.
- 5 Portable recording systems.** Establishes a new section of statute to govern use of portable recording systems.

Subdivision 1. Application; definition. Specifies that this section applies to all law enforcement agencies that maintain and use a portable recording system in investigations, or in response to emergencies, incidents, and requests for service.

Section

Definitions of “portable recording system,” “portable recording system data,” and “redact” are also provided.

Subd. 2. Data classification; court-authorized disclosure. Establishes a data classification structure for portable recording system data.

Inactive investigative data and “non-incident” data are generally private, with exceptions. Portable recording system data that are not part of an active investigation are private or nonpublic, except that the data would be public if:

- (1) the data document a peace officer’s discharge of a firearm that requires a report to the BCA;
- (2) the data document a peace officer’s use of force that results in substantial bodily harm; or
- (3) a data subject requests that the data be made public. Other data subjects who do not consent to public release must be redacted, if practicable. The activities of a law enforcement officer may not be redacted, unless the officer is working undercover.

A law enforcement agency may withhold access to portions of public data that are clearly offensive to common sensibilities. Applicable classifications of data contained in other law, such as public personnel data, would continue to apply. A Tennessean warning would not be required prior to collection of portable recording system data.

Active criminal investigative data are confidential. Active investigative data would retain the classification structure that applies to all other active investigative data under current law: the data would be confidential or protected nonpublic while the investigation is active, but subject to release by court order. This classification means that data subjects are not permitted access to the data, while the investigation is active (however, a subject would likely be provided access after being charged with a crime, based on the rules of evidence that apply in court proceedings).

A court may authorize release of portable recording system data that are private. Any person may seek a court order authorizing release of private or nonpublic portable recording system data. This includes a challenge to a law enforcement agency’s determination that the data should not be released because they are offensive to common sensibilities. In determining whether to order release, the court must consider whether the benefit to the person seeking the release outweighs the harm to the public, to the law enforcement agency, or to a data subject.

Subd. 3. Retention of data. Establishes data retention requirements for portable recording system data. In general, the data would be retained according to the law enforcement agency’s records retention schedule.

“Non-incident” data would be retained for at least 90 days. Data that would become public under the classifications in this bill, and any data related to an incident where a complaint is filed against the officer, must be retained for at least one year.

A data subject is permitted to request a longer retention period for possible evidentiary or exculpatory use of the data. Law enforcement is also permitted to retain

Section

investigative data beyond the retention schedule for possible evidentiary or exculpatory use.

Subd. 4. Access by data subjects. Establishes certain rights for subjects of portable recording system data.

Paragraph (a) establishes that a data subject includes the peace officer who collected the data, and any other individual or entity, including other officers, whose image or voice is included on the recording.

Paragraph (b) grants data subjects access to the data to the full extent required by chapter 13 as long as the data is retained. A data subject who does not consent to release must be redacted, if another subject of the data requests access. The identity and activities of an on-duty officer may not be redacted, unless the officer is working undercover.

Paragraph (c) permits peace officers to review the data, unrestricted and in its original form, prior to completing a written report or formal statement on the officer's investigation or response.

Subd. 5. Inventory of portable recording system technology. Requires law enforcement agencies to maintain a public record of portable recording system usage, including the number of devices owned or maintained by the agency, a daily record of the number deployed, and other specified information related to the amount of data collected and the agency's policies for use.

Subd. 6. Use of agency-issued portable recording systems. Prohibits an on-duty peace officer from using any portable recording system other than the system issued by the officer's agency.

Subd. 7. Authorization to access data. Provides standards for law enforcement agencies in regulating how portable recording system data may be accessed by officers and staff of the agency. The standards include a requirement that access be limited only to legitimate specified law enforcement purposes.

Subd. 8. Sharing among agencies. Provides standards for sharing or disseminating portable recording system data among other law enforcement agencies, government entities, or with the federal government, including a requirement that the receiving agency or entity meets the standards for access provided in subdivision 7.

These sharing and dissemination standards are identical to those enacted in 2015 related to sharing and dissemination of automated license plate reader data.

Subd. 9. Biennial audit. Requires law enforcement agencies to maintain certain records related to collection of portable recording system data, and arrange for an independent, biennial audit of the agency's compliance with the law. The governing body with jurisdiction over the agency's budget would be permitted to order an agency to suspend use of a portable recording system if the audits reveal a pattern of substantial noncompliance with the law. Audit reports must be submitted to the legislature's Data Practices Commission.

Subd. 10. Notification to BCA. Requires an agency to provide notice to the BCA within ten days of obtaining any new technology that expands the surveillance capacity

Section

of a portable recording system beyond audio and video recording. The notice is public and must be posted on the BCA's website.

Subd. 11. Portable recording system vendor. Clarifies that vendors who provide services to a law enforcement agency related to portable recording systems (such as hosting data storage in the cloud) must comply with all of the requirements of the Data Practices Act, and are subject to additional penalties for improper disclosure of data.

Subd. 10. Penalties for violation. Establishes enhanced penalties for a law enforcement agency that willfully violates a requirement of this section. The penalty range for willful violations provided in current law would be doubled—from a range of \$1,000 to \$15,000 per violation, to \$2,000 to \$30,000 per violation.

Effective date. This section would be effective August 1, 2016. An agency that maintains data that would be beyond the retention schedule provided in this section must destroy the data within 15 days of the effective date.

6 Portable recording systems adoption; written policy required. This section provides standards for public comment on implementation of a portable recording system within a jurisdiction, requires adoption of written policies and procedures to govern the system's use, and establishes the minimum content requirements for those policies and procedures.

Subdivision 1. Definition. Provides a technical cross-reference to the definition of "portable recording system" provided in chapter 13.

Subd. 2. Public comment. Requires law enforcement agencies to provide an opportunity to provide public comment on adoption or implementation of a portable recording system. The agency must accept written comments, and provide an opportunity for comment at a regularly-scheduled meeting of the governing body with jurisdiction over the agency.

Subd. 3. Written policies and procedures required. Requires the chief officer of a law enforcement agency that proposes to use a portable recording system to adopt a written policy governing its use. An opportunity for public comment must be provided, and the final policy is must be maintained on the agency's website. A list of the issues that must be addressed in the policy are provided in the bill.

Effective date. This section is effective August 1, 2016. Agencies currently using a portable recording system as of the effective date must adopt a policy governing use no later than January 15, 2017.

7 Legislative auditor review. Provides for a comprehensive review of agency compliance with the requirements established by this bill, to be conducted by the legislative auditor in 2019. A report to the legislature is requested by January 15, 2020.