CHAPTER 171--S.F.No. 498

An act relating to data practices; classifying portable recording system data; establishing requirements for the destruction of data; requiring written policies and procedures; imposing requirements on vendors; providing for damage awards; requiring a legislative auditor review;amending Minnesota Statutes 2014, section 13.82, subdivisions 6, 7, 15; Minnesota Statutes 2015 Supplement, section 13.82, subdivision 2; proposing coding for new law in Minnesota Statutes, chapters 13; 626.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 2015 Supplement, section 13.82, subdivision 2, is amended to read:

Subd. 2. **Arrest data.** The following data created or collected by law enforcement agencies which document any actions taken by them to cite, arrest, incarcerate or otherwise substantially deprive an adult individual of liberty shall be public at all times in the originating agency:

(a) time, date and place of the action;

(b) any resistance encountered by the agency;

(c) any pursuit engaged in by the agency;

(d) whether any weapons were used by the agency or other individual;

(e) the charge, arrest or search warrants, or other legal basis for the action;

(f) the identities of the agencies, units within the agencies and individual persons taking the action;

(g) whether and where the individual is being held in custody or is being incarcerated by the agency;

(h) the date, time and legal basis for any transfer of custody and the identity of the agency or person who received custody;

(i) the date, time and legal basis for any release from custody or incarceration;

(j) the name, age, sex and last known address of an adult person or the age and sex of any juvenile person cited, arrested, incarcerated or otherwise substantially deprived of liberty;

(k) whether the agency employed ~~an~~ a portable recording system, automated license plate reader, wiretaps or other eavesdropping techniques, unless the release of this specific data would jeopardize an ongoing investigation;

(l) the manner in which the agencies received the information that led to the arrest and the names of individuals who supplied the information unless the identities of those individuals qualify for protection under subdivision 17; and

(m) response or incident report number.

Sec. 2. Minnesota Statutes 2014, section 13.82, subdivision 6, is amended to read:

Subd. 6. **Response or incident data.** The following data created or collected by law enforcement agencies which document the agency's response to a request for service including, but not limited to, responses to traffic accidents, or which describe actions taken by the agency on its own initiative shall be public government data:

(a) date, time and place of the action;

(b) agencies, units of agencies and individual agency personnel participating in the action unless the identities of agency personnel qualify for protection under subdivision 17;

(c) any resistance encountered by the agency;

(d) any pursuit engaged in by the agency;

(e) whether any weapons were used by the agency or other individuals;

(f) a brief factual reconstruction of events associated with the action;

(g) names and addresses of witnesses to the agency action or the incident unless the identity of any witness qualifies for protection under subdivision 17;

(h) names and addresses of any victims or casualties unless the identities of those individuals qualify for protection under subdivision 17;

(i) the name and location of the health care facility to which victims or casualties were taken;

(j) response or incident report number;

(k) dates of birth of the parties involved in a traffic accident;

(l) whether the parties involved were wearing seat belts; ~~and~~

(m) the alcohol concentration of each driver; and

(n) whether the agency used a portable recording system to document the agency's response or actions.

Sec. 3. Minnesota Statutes 2014, section 13.82, subdivision 7, is amended to read:

Subd. 7. **Criminal investigative data.** Except for the data defined in subdivisions 2, 3, and 6, investigative data collected or created by a law enforcement agency in order to prepare a case against a person, whether known or unknown, for the commission of a crime or other offense for which the agency has primary investigative responsibility are confidential or protected nonpublic while the investigation is active. Inactive investigative data are public unless the release of the data would jeopardize another ongoing investigation or would reveal the identity of individuals protected under subdivision 17. Images and recordings, including photographs, video, and audio records, which are part of inactive investigative files and which are clearly offensive to common sensibilities are classified as private or nonpublic data, provided that the existence of the ~~photographs~~ images and recordings shall be disclosed to any person requesting access to the inactive investigative file. An investigation becomes inactive upon the occurrence of any of the following events:

(a) a decision by the agency or appropriate prosecutorial authority not to pursue the case;

(b) expiration of the time to bring a charge or file a complaint under the applicable statute of limitations, or 30 years after the commission of the offense, whichever comes earliest; or

(c) exhaustion of or expiration of all rights of appeal by a person convicted on the basis of the investigative data.

Any investigative data presented as evidence in court shall be public. Data determined to be inactive under clause (a) may become active if the agency or appropriate prosecutorial authority decides to renew the investigation.

During the time when an investigation is active, any person may bring an action in the district court located in the county where the data are being maintained to authorize disclosure of investigative data. The court may order that all or part of the data relating to a particular investigation be released to the public or to the person bringing the action. In making the determination as to whether investigative data shall be disclosed, the court shall consider whether the benefit to the person bringing the action or to the public outweighs any harm to the public, to the agency or to any person identified in the data. The data in dispute shall be examined by the court in camera.

Sec. 4. Minnesota Statutes 2014, section 13.82, subdivision 15, is amended to read:

Subd. 15. **Public benefit data.** Any law enforcement agency may make any data classified as confidential or protected nonpublic pursuant to subdivision 7 or as private or nonpublic under section 13.825 accessible to any person, agency, or the public if the agency determines that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest.

Sec. 5. **[13.825] PORTABLE RECORDING SYSTEMS.**

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

(b) As used in this section:

(1) "portable recording system" means a device worn by a peace officer that is capable of both video and audio recording of the officer's activities and interactions with others or collecting digital multimedia evidence as part of an investigation;

(2) "portable recording system data" means audio or video data collected by a portable recording system; and

(3) "redact" means to blur video or distort audio so that the identity of the subject in a recording is obscured sufficiently to render the subject unidentifiable.

Subd. 2. **Data classification; court-authorized disclosure.** (a) Data collected by a portable recording system are private data on individuals or nonpublic data, subject to the following:

(1) data that document the discharge of a firearm by a peace officer in the course of duty, if a notice is required under section 626.553, subdivision 2, or the use of force by a peace officer that results in substantial bodily harm, as defined in section 609.02, subdivision 7a, are public;

(2) data are public if a subject of the data requests it be made accessible to the public, except that, if practicable, (i) data on a subject who is not a peace officer and who does not consent to the release must be redacted, and (ii) data on a peace officer whose identity is protected under section 13.82, subdivision 17, clause (a), must be redacted;

(3) portable recording system data that are active criminal investigative data are governed by section 13.82, subdivision 7, and portable recording system data that are inactive criminal investigative data are governed by this section;

(4) portable recording system data that are public personnel data under section 13.43, subdivision 2, clause (5), are public; and

(5) data that are not public data under other provisions of this chapter retain that classification.

(b) A law enforcement agency may redact or withhold access to portions of data that are public under this subdivision if those portions of data are clearly offensive to common sensibilities.

(c) Section 13.04, subdivision 2, does not apply to collection of data classified by this subdivision.

(d) Any person may bring an action in the district court located in the county where portable recording system data are being maintained to authorize disclosure of data that are private or nonpublic under this section or to challenge a determination under paragraph (b) to redact or withhold access to portions of data because the data are clearly offensive to common sensibilities. The person bringing the action must give notice of the action to the law enforcement agency and subjects of the data, if known. The law enforcement agency must give notice to other subjects of the data, if known, who did not receive the notice from the person bringing the action. The court may order that all or part of the data be released to the public or to the person bringing the action. In making this determination, the court shall consider whether the benefit to the person bringing the action or to the public outweighs any harm to the public, to the law enforcement agency, or to a subject of the data and, if the action is challenging a determination under paragraph (b), whether the data are clearly offensive to common sensibilities. The data in dispute must be examined by the court in camera. This paragraph does not affect the right of a defendant in a criminal proceeding to obtain access to portable recording system data under the Rules of Criminal Procedure.

Subd. 3. **Retention of data.** (a) Portable recording system data that are not active or inactive criminal investigative data and are not described in paragraph (b) must be maintained for at least 90 days and destroyed according to the agency's records retention schedule approved pursuant to section 138.17.

(b) Portable recording system data must be maintained for at least one year and destroyed according to the agency's records retention schedule approved pursuant to section 138.17 if:

(1) the data document (i) the discharge of a firearm by a peace officer in the course of duty if a notice is required under section 626.553, subdivision 2, or (ii) the use of force by a peace officer that results in substantial bodily harm; or

(2) a formal complaint is made against a peace officer related to the incident.

(c) If a subject of the data submits a written request to the law enforcement agency to retain the recording beyond the applicable retention period for possible evidentiary or exculpatory use related to the circumstances under which the data were collected, the law enforcement agency shall retain the recording for an additional time period requested by the subject of up to 180 days and notify the requester that the recording will then be destroyed unless a new request is made under this paragraph.

(d) Notwithstanding paragraph (b) or (c), a government entity may retain a recording for as long as reasonably necessary for possible evidentiary or exculpatory use related to the incident with respect to which the data were collected.

Subd. 4. **Access by data subjects.** (a) For purposes of this chapter, a portable recording system data subject includes the peace officer who collected the data, and any other individual or entity, including any other peace officer, regardless of whether the officer is or can be identified by the recording, whose image or voice is documented in the data.

(b) An individual who is the subject of portable recording system data has access to the data, including data on other individuals who are the subject of the recording. If the individual requests a copy of the recording, data on other individuals who do not consent to its release must be redacted from the copy. The identity and activities of an on-duty peace officer engaged in an investigation or response to an emergency, incident, or request for service may not be redacted, unless the officer's identity is subject to protection under section 13.82, subdivision 17, clause (a).

Subd. 5. **Inventory of portable recording system technology.** A law enforcement agency that uses a portable recording system must maintain the following information, which is public data:

(1) the total number of recording devices owned or maintained by the agency;

(2) a daily record of the total number of recording devices actually deployed and used by officers and, if applicable, the precincts in which they were used;

(3) the policies and procedures for use of portable recording systems required by section 626.8473; and

(4) the total amount of recorded audio and video data collected by the portable recording system and maintained by the agency, the agency's retention schedule for the data, and the agency's procedures for destruction of the data.

Subd. 6. **Use of agency-issued portable recording systems.** While on duty, a peace officer may only use a portable recording system issued and maintained by the officer's agency in documenting the officer's activities.

Subd. 7. **Authorization to access data.** (a) A law enforcement agency must comply with sections 13.05, subdivision 5, and 13.055 in the operation of portable recording systems and in maintaining portable recording system data.

(b) The responsible authority for a law enforcement agency must establish written procedures to ensure that law enforcement personnel have access to the portable recording system data that are not public only if authorized in writing by the chief of police, sheriff, or head of the law enforcement agency, or their designee, to obtain access to the data for a legitimate, specified law enforcement purpose.

Subd. 8. **Sharing among agencies.** (a) Portable recording system data that are not public may only be shared with or disseminated to another law enforcement agency, a government entity, or a federal agency upon meeting the standards for requesting access to data as provided in subdivision 7.

(b) If data collected by a portable recording system are shared with another state or local law enforcement agency under this subdivision, the agency that receives the data must comply with all data classification, destruction, and security requirements of this section.

(c) Portable recording system data may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by this section or other applicable law.

Subd. 9. **Biennial audit.** (a) A law enforcement agency must maintain records showing the date and time portable recording system data were collected and the applicable classification of the data. The law enforcement agency shall arrange for an independent, biennial audit of the data to determine whether data are appropriately classified according to this section, how the data are used, and whether the data are destroyed as required under this section, and to verify compliance with subdivisions 7 and 8. If the governing body with jurisdiction over the budget of the agency determines that the agency is not complying with this section or other applicable law, the governing body may order additional independent audits. Data in the records required under this paragraph are classified as provided in subdivision 2.

(b) The results of the audit are public, except for data that are otherwise classified under law. The governing body with jurisdiction over the budget of the law enforcement agency shall review the results of the audit. If the governing body determines that there is a pattern of substantial noncompliance with this section, the governing body must order that operation of all portable recording systems be suspended until the governing body has authorized the agency to reinstate their use. An order of suspension under this paragraph may only be made following review of the results of the audit and review of the applicable provisions of this chapter, and after providing the agency and members of the public a reasonable opportunity to respond to the audit's findings in a public meeting.

(c) A report summarizing the results of each audit must be provided to the governing body with jurisdiction over the budget of the law enforcement agency and to the Legislative Commission on Data Practices and Personal Data Privacy no later than 60 days following completion of the audit.

Subd. 10. **Notification to BCA.** Within ten days of obtaining new surveillance technology that expands the type or scope of surveillance capability of a portable recording system device beyond video or audio recording, a law enforcement agency must notify the Bureau of Criminal Apprehension that it has obtained the new surveillance technology. The notice must include a description of the technology and its surveillance capability and intended uses. The notices are accessible to the public and must be available on the bureau's Web site.

Subd. 11. **Portable recording system vendor.** (a) For purposes of this subdivision, "portable recording system vendor" means a person who is not a government entity and who provides services for the creation, collection, retention, maintenance, processing, or dissemination of portable recording system data for a law enforcement agency or other government entity. By providing these services to a government entity, a vendor is subject to all of the requirements of this chapter as if it were a government entity.

(b) A portable recording system vendor that stores portable recording system data in the cloud must protect the data in accordance with the security requirements of the United States Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy 5.4 or its successor version.

(c) Subject to paragraph (d), in an action against a vendor under section 13.08 for a violation of this chapter, the vendor is liable for presumed damages of $2,500 or actual damages, whichever is greater, and reasonable attorney fees.

(d) In an action against a vendor that improperly discloses data made not public by this chapter or any other statute classifying data as not public, the vendor is liable for presumed damages of $10,000 or actual damages, whichever is greater, and reasonable attorney fees.

Subd. 12. **Penalties for violation.** In addition to any other remedies provided by law, in the case of a willful violation of this section a law enforcement agency is subject to exemplary damages of not less than twice the minimum, nor more than twice the maximum allowable for exemplary damages under section 13.08, subdivision 1.

EFFECTIVE DATE. This section is effective August 1, 2016. Data collected before the effective date of this section must be destroyed, if required by this section, no later than 15 days after the date this section becomes effective.

Sec. 6. **[626.8473] PORTABLE RECORDING SYSTEMS ADOPTION; WRITTEN POLICY REQUIRED.**

Subdivision 1. **Definition.** As used in this section, "portable recording system" has the meaning provided in section 13.825, subdivision 1.

Subd. 2. **Public comment.** A local law enforcement agency must provide an opportunity for public comment before it purchases or implements a portable recording system. At a minimum, the agency must accept public comments submitted electronically or by mail, and the governing body with jurisdiction over the budget of the law enforcement agency must provide an opportunity for public comment at a regularly-scheduled meeting.

Subd. 3. **Written policies and procedures required.** (a) The chief officer of every state and local law enforcement agency that uses or proposes to use a portable recording system must establish and enforce a written policy governing its use. In developing and adopting the policy, the law enforcement agency must provide for public comment and input as provided in subdivision 2. Use of a portable recording system without adoption of a written policy meeting the requirements of this section is prohibited. The written policy must be posted on the agency's Web site, if the agency has a Web site.

(b) At a minimum, the written policy must incorporate the following:

(1) the requirements of section 13.825 and other data classifications, access procedures, retention policies, and data security safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;

(2) procedures for testing the portable recording system to ensure adequate functioning;

(3) procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;

(4) circumstances under which recording is mandatory, prohibited, or at the discretion of the officer using the system;

(5) circumstances under which a data subject must be given notice of a recording;

(6) circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;

(7) procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and

(8) procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

EFFECTIVE DATE. This section is effective August 1, 2016, provided that a law enforcement agency using a portable recording system on that date must adopt the policy required under this section no later than January 15, 2017.

Sec. 7. **LEGISLATIVE AUDITOR REVIEW.**

Beginning no earlier than January 1, 2019, the legislative auditor is requested to conduct a comprehensive review of compliance with the requirements of Minnesota Statutes, sections 13.825 and 626.8473. Data used for purposes of the review must include the results of the biennial audits required by Minnesota Statutes, section 13.825, subdivision 9, and may also include any other data that, in the judgment of the legislative auditor, assists in developing a complete understanding of any compliance or implementation issues resulting from enactment of those sections. The legislative auditor is requested to submit the results of the comprehensive review to the legislature no later than January 15, 2020.

Presented to the governor May 24, 2016