State of Minnesota

HOUSE OF REPRESENTATIVES

EIGHTY-NINTH SESSION

H. F. No. 3468

03/23/2016 Authored by Scott; Lesch; Metsa; Anderson, M., and Backer
The bill was read for the first time and referred to the Committee on Civil Law and Data Practices

A bill for an act

relating to data practices; classifying portable recording system data; establishing requirements for destruction of certain data in certain cases; requiring consent to record data on private property with exceptions; imposing requirements on law enforcement agencies and vendors; requiring audits; requiring a written policy; requiring approval by a local governing body; amending Minnesota Statutes 2014, section 13.82, subdivisions 6, 7; 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, including a brief description of its compliance with section 13.825, subdivision 3.

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

Subdivision 1. **Application; definitions.** (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) A peace officer who collects portable recording system data, and any other officer whose activities are recorded on the data, regardless of whether the officer is or can be identified by the recording, is a subject of the data for purposes of this chapter, except that the rights of a data subject provided in subdivisions 2 and 3 do not apply to a peace officer while the officer is investigating or responding to an emergency, incident, or request for service.

(c) As used in this section, "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.

Subd. 2. **Data classification; retention requirements.** (a) Data collected by a portable recording system are classified and must be maintained as follows:

(1) data that document law enforcement activity that does not constitute an investigation or a response to an emergency, incident, or request for service, are private or nonpublic data, and must be destroyed within 30 days of collection;

(2) data that document a law enforcement investigation or response to an emergency, incident, or request for service are public, subject to paragraph (c), if the data document activities in a location where a subject of the data does not have a reasonable expectation of privacy. The data must be retained for no longer than any applicable statute of limitations period has expired, or 180 days after the close of an investigation, whichever is later; and

(3) data that document a law enforcement investigation or response to an emergency, incident, or request for service are private data on individuals or nonpublic data if the data document activities in a location where a subject of the data has a reasonable expectation of privacy, except that data that document a law enforcement investigation or response that involves a use of force resulting in bodily harm, as defined in section 609.02, are public, subject to paragraph (c). Data subject to this clause must be retained for no longer than any applicable statute of limitations period has expired, or 180 days after the close of an investigation, whichever is later.

(b) Data subject to the classification and retention requirements of this subdivision may not be released or disseminated to any person unless the following individuals' identities have been blurred or distorted sufficiently to render the individuals unidentifiable:

(1) individuals whose appearance on the recording are incidental and whose activities are unrelated to the purpose of the law enforcement investigation or response; and

(2) individuals whose identities are subject to protection under section 13.82.

(c) Portable recording system data that relate to an active investigation are classified as provided in section 13.82, subdivision 7. When the investigation becomes inactive, the data are classified as provided in this subdivision.

Subd. 3. **Notice and consent required to collect data in private locations; exceptions.** (a) Except as provided in paragraph (b), a portable recording system may not record activity at a location where a subject of the data has a reasonable expectation of privacy unless:

(1) the peace officer has notified each data subject whose activities may be recorded of the existence of the recording system; and

(2) each data subject has consented to the recording system's use.

(b) The notice and consent requirements of paragraph (a) are not required:

(1) in searches conducted according to the terms of a valid search warrant;

(2) where exigent circumstances reasonably prevent the law enforcement agency from providing notice and obtaining consent; or

(3) from individuals recorded incidentally by the portable recording system and whose activities are unrelated to the purpose of the law enforcement investigation or response, if the officer has made a reasonable effort to prevent those activities from being recorded.

(c) The consent requirements of paragraph (a) are not required in an investigation of, or response to, a report of domestic abuse as defined in section 518B.01, subdivision 2.

Subd. 4. **Use of portable recording systems required.** (a) At any time an officer is equipped with a portable recording system, the system must be used to document the peace officer's investigations and responses to all emergencies, incidents, and requests for service. The portable recording system must collect data for the full duration of the officer's investigation or response, subject to the notice and consent requirements of subdivision 3. A peace officer may only use a portable recording system issued and maintained by the officer's agency documenting the officer's investigations and responses.

(b) In the event of a conflict between this subdivision and subdivision 7, this subdivision applies.

Subd. 5. **Facial recognition technology.** A law enforcement agency may not deploy or use facial recognition technology in connection with any portable recording system data unless expressly authorized by law. Facial recognition technology may be used to blur or distort the identity of an individual protected by subdivision 2, paragraph (b).

Subd. 6. **Use of force cases; officer review prior to completion of report prohibited.** A responding peace officer may not review data collected on a portable

recording system prior to completing the officer's final report documenting the emergency, incident, or request for service if the law enforcement response involved a use of force.

Subd. 7. **First amendment activities.** To the extent possible, portable recording systems must only be used to record a peace officer's investigations and responses to a specific emergency, incident, or request for service. Except in response to a specific emergency, incident, or request for service, a portable recording system may not collect data at any event, activity, or assembly subject to protection under the First Amendment of the United States Constitution unless the data collection has been authorized, in writing, by the chief of police, sheriff, or head of the law enforcement agency. A written authorization is public data at all times.

Subd. 8. **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 subject to the terms of a search warrant. Consistent with the requirements of paragraph (c), each access must include a record of the search warrant that is the basis for the access.

(c) The ability of authorized individuals to enter, update, or access portable recording system data must be limited through the use of role-based access that corresponds to the official duties or training level of the individual and the statutory authorization that grants access for that purpose. All queries and responses, and all actions in which data are entered, updated, accessed, shared, or disseminated, must be recorded in a data audit trail. Data contained in the audit trail are public, to the extent that the data are not otherwise classified by law.

Subd. 9. **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 subject to a search warrant and upon meeting the standards for requesting access to data as provided in subdivision 8.

(b) If data collected by a portable recording system are shared with another 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. 10. **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 they are destroyed as required under this section, and to verify compliance with subdivisions 8 and 9. If the commissioner of administration believes that a law enforcement agency is not complying with this section or other applicable law, the commissioner may order a law enforcement agency to arrange for 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. The commissioner of administration shall review the results of the audit. If the commissioner determines that there is a pattern of substantial noncompliance with this section by the law enforcement agency, the agency must immediately suspend operation of all portable recording systems until the commissioner has authorized the agency to reinstate their use. An order of suspension under this paragraph may be issued by the commissioner upon review of the results of the audit, upon review of the applicable provisions of this chapter, and after providing the agency a reasonable opportunity to respond to the audit's findings.

(c) A report summarizing the results of each audit must be provided to the commissioner of administration, to the chair and ranking minority members of the committees of the house of representatives and the senate with jurisdiction over data practices and public safety issues, and to the Legislative Commission on Data Practices and Personal Data Privacy no later than 30 days following completion of the audit.

Subd. 11. **Notification to Bureau of Criminal Apprehension.** (a) Within ten days of implementation of a portable recording system, a law enforcement agency must notify the Bureau of Criminal Apprehension of that implementation, including the number of officers equipped with a portable recording system device.

(b) The Bureau of Criminal Apprehension must maintain a list of law enforcement agencies using portable recording systems and the number of officers in each agency using a portable recording system device. The list is public and must be available on the bureau's Web site.

Subd. 12. **Portable recording system vendors.** (a) For purposes of this subdivision, a "portable recording system vendor" means a person who is not a government entity and that 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) Subject to paragraph (c), 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.

(c) 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.

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. 5. **[626.8473] PORTABLE RECORDING SYSTEMS ADOPTION; WRITTEN POLICY REQUIRED.**

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

Subd. 2. **Public comment; approval of local governing body required.** (a) A local law enforcement agency may not purchase or implement a portable recording system unless the governing body with jurisdiction over the law enforcement agency has approved:

(1) purchase and implementation of the system; and

(2) the written policy required under subdivision 3.

(b) A vote to approve use of a portable recording system and the written policy required by subdivision 3 must occur at a regularly scheduled meeting of the governing body, following an opportunity for public comment. Notice of the meeting must be posted at least 30 days prior to the date of the 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, subject to the approval requirements in subdivision 2. Use of a portable recording system without adoption of a written policy meeting the requirements of this subdivision is prohibited. The written policy must be posted on the agency's 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 the consent of a data subject is required prior to recording;

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

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

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

(9) 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; and

(10) if applicable, any other standards for use contained in a uniform policy adopted by the Minnesota Chiefs of Police Association or the Minnesota Sheriffs' Association.

EFFECTIVE DATE. This section is effective August 1, 2016, provided that a law enforcement agency using a portable recording system on that date must secure the governing body's approval of the system and the policy required under this section, no later than January 15, 2017.