State of Minnesota

HOUSE OF REPRESENTATIVES

EIGHTY-SIXTH SESSION

HOUSE FILE NO. 1449

March 9, 2009
Authored by Lesch
The bill was read for the first time and referred to the Committee on Public Safety Policy and Oversight

A bill for an act

relating to public safety; classifying criminal intelligence data under the Data Practices Act; proposing coding for new law in Minnesota Statutes, chapter 13.

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

Section 1. **[13.823] CRIMINAL INTELLIGENCE DATA.**

Subdivision 1. **Definitions.** The terms defined in this section have the meanings given them.

(a) "Association data" means data that document the associations or activities of a person and that are about that person's political, religious, or social views.

(b) "Criminal intelligence data" means data a law enforcement agency uses to anticipate, prevent, or monitor possible criminal or terrorist activity by a person. Criminal intelligence data does not include association data unless the association data have a direct relationship to criminal or terrorist activities by a person.

(c) "Criminal intelligence data assessment" means an analysis based on criminal intelligence data.

(d) "Criminal predicate" means sufficient, articulable facts, along with rational inferences from those facts, to give employees working under the supervision of a law enforcement agency a basis to believe that there is a reasonable possibility that a person is involved in criminal or terrorist activity.

(e) "Critical infrastructure" means physical or virtual assets that, when incapacitated or destroyed, would have a debilitating impact on the physical or economic security, public health, or public safety of the citizens of the state.

(f) "Law enforcement agency" means a government agency at the federal, state, or local level, including agencies in other states, that are charged with detecting criminal activity, enforcing criminal laws, or protecting critical infrastructure.

(g) "Terrorist activity" means acts dangerous to human life that violate the criminal laws of this state or the United States and appear to be intended to:

(1) intimidate or coerce the civilian population;

(2) influence the policy of the state by intimidation or coercion; or

(3) affect the state by mass destruction, assassination, or kidnapping.

(h) "Threat of imminent serious harm" means a credible impending threat to the safety of a person, government entity, or property.

Subd. 2. **Data classification and retention.** (a) Criminal intelligence data are classified as confidential data on individuals or protected nonpublic data for a period of one year. After one year, the data classification changes to private data on individuals or nonpublic data unless the following criteria are met:

(1) the source of the data is reliable and verifiable;

(2) the person alleged to be involved in criminal activity can be identified;

(3) the allegations of criminal activity are supported by a criminal predicate;

(4) the data were collected in a lawful manner; and

(5) the data are accurate and current.

If the criteria are met, the data remain classified as confidential data on individuals or protected nonpublic data.

(b) The informed consent of the subject of the data is not effective if the data are classified as private data on individuals or nonpublic data.

(c) Notwithstanding any other law to the contrary, data that have changed classification as required by paragraph (a) shall not be maintained by a government entity for more than three years from the last date the classification changed.

(d) If, prior to the destruction required by paragraph (c), the criteria in paragraph (a) can be met, the data classification reverts to confidential data on individuals or protected nonpublic data.

(e) Criminal intelligence data assessments and dissemination records are classified as confidential data on individuals or protected nonpublic data.

Subd. 3. **Sharing authorized.** (a) Criminal intelligence data may be shared with:

(1) a law enforcement agency, if the recipient demonstrates a criminal predicate related to the data requested;

(2) a law enforcement agency to charge a person with a crime or allege that a juvenile is delinquent;

(3) a person or government entity when the dissemination is needed to protect the person, government entity, or property from the threat of imminent serious harm;

(4) a person or government entity to protect critical infrastructure;

(5) a law enforcement agency conducting the background check required by section 626.87; or

(6) the public to promote public health or safety or to dispel widespread rumor or unrest.

(b) Criminal intelligence data assessments may be shared with:

(1) a law enforcement agency;

(2) a person or government entity when the dissemination is needed to protect the person, government entity, or property from the threat of imminent serious harm;

(3) a person or government entity to protect critical infrastructure; or

(4) the public to promote public health or safety or to dispel widespread rumor or unrest.

Subd. 4. **Data prohibitions.** (a) Unless there is a criminal predicate, a law enforcement agency may not maintain or use criminal intelligence data.

(b) Association data may not be maintained by a Minnesota law enforcement agency or shared with any law enforcement agency.

Subd. 5. **Dissemination record.** A law enforcement agency shall keep a dissemination record of each sharing made under subdivision 3, paragraph (a).