State of Minnesota

HOUSE OF REPRESENTATIVES

EIGHTY-SEVENTH SESSION

H. F. No. 2470

02/23/2012 Authored by Cornish, Kelly, Lesch and Peterson, S.,
The bill was read for the first time and referred to the Committee on Public Safety and Crime Prevention Policy and Finance
03/14/2012 Adoption of Report: Re-referred to the Committee on Civil Law without further recommendation

A bill for an act

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

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

Section 1. **[13.824] CRIMINAL INTELLIGENCE DATA.**

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

(b) "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.

(c) "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.

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

(e) "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.

(f) "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.

(g) "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.

(h) "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.

(i) "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).

Sec. 2. **[13.8735] CRIMINAL INTELLIGENCE SYSTEMS.**

Subdivision 1. **Definitions.** (a) For purposes of this section, the terms in this subdivision have the meanings given them.

(b) "Criminal intelligence data" means data that has been evaluated to determine that it:

(1) is relevant to the identification of and the criminal activity engaged in by an individual or organization reasonably suspected of involvement in criminal activity; and

(2) meets criminal intelligence system submission criteria.

(c) "Criminal intelligence system" or "intelligence system" means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence data.

(d) "Intelligence project" or "project" means the organizational unit that operates an intelligence system on behalf of and for the benefit of a single agency or the organization that operates an interjurisdictional intelligence system on behalf of a group of participating agencies.

(e) "Interjurisdictional intelligence system" means an intelligence system that involves two or more participating agencies representing different government entities or jurisdictions.

(f) "Participating agency" means an agency of local, county, state, federal, or other governmental unit that exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence data through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system.

(g) "Validation of data" means the procedures governing the periodic review of criminal intelligence data to assure its continuing compliance with system submission criteria established by regulation or program policy.

Subd. 2. **Operating principles.** (a) A project shall collect and maintain criminal intelligence data concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence data about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless the data directly relates to criminal conduct or activity and there is reasonable suspicion that the data subject is or may be involved in criminal conduct or activity.

(c) Reasonable suspicion or criminal predicate is established when data exists that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting data submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency that is subject to audit procedures established by subdivision 4.

(d) A project shall not include in any criminal intelligence system data that has been obtained in violation of any applicable federal, state, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of federal, state, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by subdivision 4.

(e) A project shall disseminate criminal intelligence data only where there is a need to know and a right to know the data in the performance of a law enforcement activity.

(f) A project shall disseminate criminal intelligence data only to law enforcement authorities who shall agree to follow procedures regarding data receipt, maintenance, security, and dissemination which are consistent with this section. This paragraph shall not limit the dissemination of an assessment of criminal intelligence data to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence data shall adopt administrative, technical, and physical safeguards, including audit trails, to prevent unauthorized access and against intentional or unintentional damage. A record indicating who has been given data, the reason for release of the data, and the date of each dissemination outside the project shall be kept. Data shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the "need to know" and "right to know" standards for dissemination to other agencies as provided in paragraph (e). The project is responsible for establishing the existence of an inquirer's need to know and right to know the data being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency that is subject to routine inspection and audit procedures established by the project.

(h) A project:

(1) where appropriate, must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) must restrict access to its facilities, operating environment, and documentation to organizations and personnel authorized by the project;

(3) must store data in the system in a manner that prevents the data from being modified, destroyed, accessed, or purged without authorization;

(4) must institute procedures to protect criminal intelligence data from unauthorized access, theft, sabotage, fire, flood, or other natural or man-made disaster;

(5) must adopt rules based on good cause to implement its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

(6) may authorize and utilize off-site system databases to the extent that they comply with these security requirements.

(i) All projects shall adopt procedures to ensure that all data retained by a project has relevancy and importance. The procedures shall provide for the periodic review of data and the destruction of any data that is misleading, obsolete, or otherwise unreliable, and shall require that any recipient agencies be advised of any errors or corrections. All data retained as a result of this review must identify the name of the reviewer, date of review, and explanation of the decision to retain. Data retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five years.

(j) A project must not purchase or use in the course of the project any electronic, mechanical, or other device for surveillance purposes that is in violation of sections 626A.01 to 626A.381 and the Electronic Communications Privacy Act of 1986, Public Law 99-508, United States Code, title 18, sections 2510-2520, 2701-2709, and 3121-3125.

(k) A project must not harass or interfere with any lawful political activities as part of the intelligence operation.

(l) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of data contained in the system.

(m) A participating agency of an interjurisdictional intelligence system must maintain in its agency files data that documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection as provided in subdivision 4.

Subd. 3. **Supervision.** The head of an agency, or an individual expressly delegated control and supervision by the head of the agency, maintaining an interjurisdictional criminal intelligence system shall:

(1) assume official responsibility and accountability for actions taken in the name of the joint entity; and

(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the data transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles in this chapter.

The principles in this section shall be included in bylaws or operating procedures for each system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance, and dissemination of data included as part of an interjurisdictional system.

Subd. 4. **Audit of data submitted to system; reports.** At least once every three years, the Bureau of Criminal Apprehension shall conduct periodic audits of criminal intelligence systems and interjurisdictional criminal intelligence systems for compliance

with this section. The bureau shall have access to the documenting data for purposes of conducting an audit. The bureau shall conduct the audit in a manner that protects the confidentiality and sensitivity of participating agency intelligence records. By October 1 of each year, the bureau shall submit a report on the results of the audits to the commissioner of public safety.

Subd. 5. **Classification of intelligence data.** Criminal intelligence data is classified as confidential data on individuals, or protected nonpublic data.

EFFECTIVE DATE. This section is effective August 1, 2012.