S.F. No. 3384, as introduced - 86th Legislative Session (2009-2010) [10-6347]

A bill for an act

relating to data practices; establishing operating principles for criminal intelligence databases; classifying data; 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 DATABASES.**

Subdivision 1. **Definitions.** (a) The definitions in this subdivision apply to this section.

(b) "Criminal intelligence data" means data that have been evaluated to determine that the data:

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

(2) meet 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 governmental units 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 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 information" means the procedures governing the periodic review of criminal intelligence data to ensure its continuing compliance with system submission criteria.

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

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

(c) Reasonable suspicion is established when information 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 through examination of supporting data submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency.

(d) A project must not include any criminal intelligence system data that have been obtained in violation of law. In an interjurisdictional intelligence system, the project is responsible for establishing that no data are entered in violation of law, either through examination of supporting data submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency.

Subd. 3. **Dissemination of data.** (a) A project may disseminate criminal intelligence data only if there is a need to know and a right to know the data in the performance of a law enforcement activity.

(b) A project may disseminate criminal intelligence data only to law enforcement authorities who agree to follow procedures regarding receipt, maintenance, security, and dissemination of the data that are consistent with this section. This paragraph does not limit the dissemination of an assessment of criminal intelligence data to any person, when necessary to avoid imminent danger to life or property.

Subd. 4. **Safeguards; security requirements.** A project maintaining criminal intelligence data shall ensure that administrative, technical, and physical safeguards, including audit trails, are adopted to ensure against unauthorized access and 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 must be kept. Data must be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. A project shall establish written definitions for the need-to-know and right-to-know standards for dissemination to other agencies under subdivision 3. The project is responsible for establishing the existence of an inquirer's need to know and right to know the requested data 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. An intelligence project shall ensure that the following security requirements are implemented:

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

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

(3) the project must store data in the system so that the data cannot be modified, destroyed, accessed, or purged without authorization;

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

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

(6) a project may authorize and use remote, off-premises, system databases to the extent that these databases comply with these security requirements.

Subd. 5. **Relevance.** A project shall adopt procedures to ensure that data that are retained by a project are relevant, as provided under subdivision 1, paragraph (b). These procedures must provide for the periodic review of data and the destruction of data that are misleading, obsolete, or otherwise unreliable and must require that recipient agencies be advised of changes that involve errors or corrections. Data retained after a review must reflect the name of the reviewer, the date of review, and an 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 the data's retention period, which must not be longer than five years.

Subd. 6. **Project assurances.** (a) A project shall ensure that there will be no purchase or use in the course of the project of 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, United States Code, title 18, sections 2510 to 2520, 2701 to 2709, and 3121 to 3125.

(b) A project shall establish procedures to ensure that there will be no harassment or interference with lawful political activities as part of an intelligence operation.

Subd. 7. **Data.** (a) Criminal intelligence data are confidential data on individuals.

(b) A participating agency of an interjurisdictional intelligence system must maintain data that document each submission to the system and support compliance with project entry criteria.

Subd. 8. **Supervision.** (a) The head of an agency, or an individual expressly delegated this 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 ensuring that data transmitted to the interjurisdictional intelligence system or to participating agencies will be in compliance with this section.

(b) This section must be made part of the bylaws or operating procedures for an intelligence system. Each participating agency, as a condition of participation, must accept in writing the principles that govern the submission, maintenance, and dissemination of data included as part of an interjurisdictional system.