By: McClendon H.B. No. 3324

A BILL TO BE ENTITLED

AN ACT

relating to intelligence data standards and protected personal information.

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

SECTION 1. Section 421.082, Government Code, is amended by amending Subsection (b) and adding Subsection (h) to read as follows:

(b) The center's duties include:

(1) promotion of emergency preparedness;

(2) receipt and analysis of information, assessment of threats, and issuance of public warnings related to homeland security emergencies; [~~and~~]

(3) authorization and facilitation of cooperative efforts related to emergency response and recovery efforts in the event of a homeland security emergency; and

(4) making recommendations to the Department of Public Safety regarding the monitoring of fusion centers and other criminal intelligence systems operating in this state and regarding the functions of the Texas Fusion Center Policy Council created under Section 421.083.

(h) The center may use any available revenue and may solicit and accept gifts, grants, and donations for the purposes of discharging its powers and duties under this section. The center shall use any gifts, grants, and donations received for those

purposes before using other revenue.

SECTION 2. Subchapter E, Chapter 421, Government Code, is amended by adding Section 421.083 to read as follows:

Sec. 421.083. FUSION CENTERS OPERATING IN THIS STATE: RULES AND MONITORING. (a) After considering the recommendations of the Texas Fusion Center under Section 421.082(b)(4), the Department of Public Safety shall:

(1) adopt rules to govern the operations of fusion centers and other criminal intelligence systems in this state, including guidelines to:

(A) establish a common concept of operations for any criminal intelligence systems operating in this state, in order to provide clear standards for each aspect of their activities; and

(B) inform and define the monitoring of those activities by the Texas Fusion Center Policy Council created under Subdivision (2); and

(2) create the Texas Fusion Center Policy Council to assist the department in monitoring the activities of fusion centers and other criminal intelligence systems operating in this state.

(b) The policy council is composed of one representative from each regional fusion center operating in this state.

(c) The policy council shall:

(1) develop and disseminate strategies to facilitate the implementation of applicable federal standards and programs on a statewide basis by each criminal intelligence system operating in this state;

(2) on behalf of the department and subject to the department's control, monitor the implementation of the department's common concept of operations by each criminal intelligence system operating in this state and perform audits, including financial audits, as necessary to ensure effective implementation; and

(3) recommend best practices for the operations of each criminal intelligence system, including best practices for the smooth exchange of information among those systems and best practices for the financial and budgetary operations of those systems.

(d) The department may require that a criminal intelligence system audited under this section pay any costs incurred by the policy council in relation to the audit.

(e) A member of the policy council may not receive compensation but is entitled to reimbursement for the member's travel expenses as provided by Chapter 660 and the General Appropriations Act.

SECTION 3. Chapter 421, Government Code, is amended by adding Subchapter E-1 to read as follows:

SUBCHAPTER E-1. CRIMINAL INTELLIGENCE SYSTEMS

Sec. 421.101. DEFINITIONS. In this subchapter:

(1) "Biometric information" means DNA, iris or retinal scans, palm telemetry, photographs, or facial recognition measurements or any other biometric measurements. The term does not include a thumbprint or signature.

(2) "Criminal intelligence system" means:

(A) the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange, dissemination, and analysis of criminal intelligence data; or

(B) any entity whose mission includes collecting, analyzing, or sharing intelligence data and other data for law enforcement or homeland security purposes, including the Texas Fusion Center operated by the Department of Public Safety and all regional fusion centers in this state.

(3) "Noncriminal information" means any data about persons, organizations, events, incidents, or objects, regardless of the medium in which the information exists, where no reasonable suspicion exists that a criminal activity is occurring or is about to occur.

(4) "Personally identifiable information" means all personal data and any data element or combination of data elements that identifies or could be used to identify an individual, including:

(A) an individual's:

(i) name;

(ii) date of birth;

(iii) address of residence;

(iv) electronic password;

(v) unique account number;

(vi) telephone number;

(vii) biometric information;

(viii) photograph or a description of a tattoo;

(ix) e-mail address;

(x) Internet Protocol address; or

(xi) web address; or

(B) any other unique identifier.

(5) "Protected health information" means any information about health status, provision of health care, or payment for health care services that can be linked to a specific individual.

Sec. 421.102. REASONABLE SUSPICION DEFINED. For purposes of this subchapter, reasonable suspicion is established only when information exists that establishes sufficient facts to give a trained law enforcement or criminal justice 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.

Sec. 421.103. CONDITIONS FOR TREATMENT OF INTELLIGENCE DATA AND NONCRIMINAL INFORMATION. (a) Any law enforcement or criminal justice agency, including a criminal intelligence system, that reviews, collects, submits, disseminates, discloses, or maintains intelligence data shall:

(1) review, collect, and maintain intelligence data or noncriminal information concerning an individual or organization only if:

(A) reasonable suspicion exists that the individual or organization is involved in criminal conduct or activity; and

(B) the information is relevant to that criminal

conduct or activity;

(2) disseminate intelligence data only where there is a need to know and a right to know the information in the performance of a law enforcement activity;

(3) disseminate intelligence data only to a law enforcement authority that agrees to follow procedures regarding information receipt, maintenance, security, and dissemination that are consistent with the receipt, maintenance, security, and dissemination limitations, requirements, and procedures applicable to a criminal intelligence system;

(4) provide notice to submitting criminal justice agencies, law enforcement agencies, or criminal intelligence systems or other submitting individuals before initiating formal information exchange procedures with any federal, state, or regional information system;

(5) require any agency submitting data to maintain in its agency files documentation of each submission and to make that documentation available for reasonable audit and inspection by the attorney general;

(6) adopt policies regarding screening, rejecting for employment, transferring, or removing personnel authorized to have direct access to intelligence data;

(7) adopt, implement, and maintain procedures to ensure the maximum feasible security, confidentiality, and integrity of personally identifiable information and similar data, including labeling that data to indicate:

(A) levels of sensitivity of the data;

(B) levels of confidence in the data; and

(C) the identity of a submitting criminal justice agency, law enforcement agency, or criminal intelligence system or other submitting individual;

(8)(A) adopt, implement, and maintain written information security programs governing the collection, use, dissemination, storage, retention, and destruction of personally identifiable information and similar data;

(B) ensure that criminal intelligence and other information is securely stored and protected against unauthorized access, destruction, use, modification, disclosure, or loss; and

(C) destroy the information as soon as it is no longer needed; and

(9) adopt policies and operating procedures implementing all other applicable requirements under state or federal law.

(b) Subsection (a)(3) does not limit the dissemination of an assessment of intelligence data to a government official or to any other individual if necessary to avoid imminent danger to life or property.

(c) An information security program under Subsection (a)(8)(A) must:

(1) address, without limitation, administrative, technical, and physical safeguards;

(2) include sanctions for unauthorized access, use, or disclosure of information stored and maintained in a criminal intelligence system; and

(3) comply with all federal and state privacy and information security laws and regulations, including Chapter 552.

Sec. 421.104. COLLECTION OF CERTAIN INTELLIGENCE DATA AND NONCRIMINAL INFORMATION PROHIBITED. An agency described by Section 421.103(a), including a criminal intelligence system, may not:

(1) review, collect, or maintain noncriminal information or criminal intelligence data about the political, religious, or social views, associations, military history, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless the information directly relates to criminal conduct or activity and reasonable suspicion exists that the subject of the information is or may be involved in criminal conduct or activity; or

(2) review, collect, or maintain protected health information, biometric information, or personally identifiable information unless the information directly relates to criminal conduct or activity and reasonable suspicion exists that the subject of the information is or may be involved in criminal conduct or activity.

Sec. 421.105. REPORT. (a) Not later than September 1 of each year, any law enforcement or criminal justice agency described by Section 421.103(a), including a criminal intelligence system, shall submit reports to the standing committee of each house of the legislature with primary jurisdiction over criminal justice. Each standing committee may hold a joint hearing to evaluate the reports of those agencies and may invite testimony by the agencies for that purpose.

(b) A report under this section must include:

(1) a list of all agencies requesting or submitting information or intelligence to the entity in question;

(2) a summary of any audit or review the entity underwent during the preceding year and, if the audit or review was performed for a criminal intelligence system, a summary of the methods used to investigate, evaluate, and analyze the operations of that system;

(3) the total number of requests for and responses to requests for information or intelligence; and

(4) all complaints received by the entity in relation to information collection.

Sec. 421.106. OVERSIGHT. (a) The attorney general or a designated employee of the attorney general shall provide oversight of the data and privacy protection function of criminal intelligence systems operating in this state, including the Texas Fusion Center, with regard to the collection, maintenance, and storage of personally identifiable information or intelligence data and any disclosure, transfer, or dissemination of that information or data.

(b) The attorney general or designee shall investigate, evaluate, and analyze the operations of criminal intelligence systems in this state, including the procedures of those systems, both as written and in practice, for:

(1) collecting data;

(2) protecting the privacy and security of personally identifiable information;

(3) responding to requests for information under Chapter 552; and

(4) ensuring that the activities of criminal intelligence systems do not infringe on the rights of freedom of assembly, association, and expression guaranteed by the United States Constitution and the Texas Constitution.

(c) The attorney general or designee shall examine the compliance of each criminal intelligence system in this state with this subchapter.

(d) The attorney general or designee shall examine the involvement of entities other than law enforcement or criminal justice agencies in criminal intelligence system activities and shall assess the impact of that involvement on the data and privacy protection function of criminal intelligence systems in this state.

Sec. 421.107. OVERSIGHT BOARD. (a) Each criminal intelligence system in this state shall establish and maintain an oversight board.

(b) The members of an oversight board established under this section must include:

(1) representatives from industry, law enforcement, and other related fields; and

(2) at least one privacy advocate.

Sec. 421.108. LIMITATIONS ON DISCLOSURE OF INFORMATION. Information subject to regulation by this subchapter may not be disclosed under Chapter 552 if the disclosure would:

(1) interfere with an ongoing criminal investigation or other law enforcement proceeding;

(2) constitute a clearly unwarranted invasion of personal privacy;

(3) disclose the identity of a confidential source; or

(4) endanger the life or physical safety of any individual.

SECTION 4. Subchapter F, Chapter 421, Government Code, is redesignated as Subchapter G, Chapter 421, Government Code, and amended to read as follows:

SUBCHAPTER G [~~F~~]. GOVERNOR'S INTEROPERABLE RADIO COMMUNICATIONS PROGRAM

Sec. 421.121 [~~421.095~~]. DEFINITIONS. In this subchapter:

(1) "First responder" means a public safety employee or volunteer whose duties include responding rapidly to an emergency. The term includes:

(A) a peace officer whose duties include responding rapidly to an emergency;

(B) fire protection personnel under Section 419.021;

(C) a volunteer firefighter who is:

(i) certified by the Texas Commission on Fire Protection or by the State Firemen's and Fire Marshalls' Association of Texas; or

(ii) a member of an organized volunteer fire-fighting unit as described by Section 615.003; and

(D) an individual certified as emergency medical services personnel by the Department of State Health Services.

(2) "Infrastructure equipment" means the underlying permanent equipment required to establish interoperable communication between radio systems used by local, state, and federal agencies and first responders.

Sec. 421.122 [~~421.096~~]. INTEROPERABILITY OF RADIO SYSTEMS. The office of the governor shall:

(1) develop and administer a strategic plan to design and implement a statewide integrated public safety radio communications system that promotes interoperability within and between local, state, and federal agencies and first responders;

(2) develop and administer a plan in accordance with Subdivision (1) to purchase infrastructure equipment for state and local agencies and first responders;

(3) advise representatives of entities in this state that are involved in homeland security activities with respect to interoperability; and

(4) use appropriated money, including money from relevant federal homeland security grants, for the purposes of designing, implementing, and maintaining a statewide integrated public safety radio communications system.

Sec. 421.123 [~~421.097~~]. ASSISTANCE. The office of the governor may consult with a representative of an entity described by Section 421.122(3) [~~421.096(3)~~] to obtain assistance or information necessary for the performance of any duty under this subchapter.

Sec. 421.124 [~~421.098~~]. REPORT. Not later than September 1 of each year, the office of the governor shall provide to the

legislature a report on the status of its duties under this subchapter.

SECTION 5. Section 74.151(a), Civil Practice and Remedies Code, is amended to read as follows:

(a) A person who in good faith administers emergency care is not liable in civil damages for an act performed during the emergency unless the act is wilfully or wantonly negligent, including a person who:

(1) administers emergency care using an automated external defibrillator; or

(2) administers emergency care as a volunteer who is a first responder as the term is defined under Section 421.121 [~~421.095~~], Government Code.

SECTION 6. This Act takes effect immediately if it receives a vote of two-thirds of all the members elected to each house, as provided by Section 39, Article III, Texas Constitution. If this Act does not receive the vote necessary for immediate effect, this Act takes effect September 1, 2011.