SENATE DOCKET, NO. 1449 FILED ON: 1/21/2011

SENATE . . . . . No. 1194

The Commonwealth of Massachusetts

PRESENTED BY:

Harriette L. Chandler

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act to protect privacy and personal data.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
Harriette L. Chandler	
Cynthia S. Creem	
Kenneth J. Donnelly	
James B. Eldridge	
Susan C. Fargo	
Thomas M. McGee	*Third Essex*
Karen E. Spilka	
Jennifer E. Benson	*37th Middlesex*
Steven L. Levy	*4th Middlesex*
Martha M. Walz	*8th Suffolk*

SENATE DOCKET, NO. 1449 FILED ON: 1/21/2011

SENATE . . . . . No. 1194

By Ms. Chandler, petition (accompanied by bill, Senate, No. 1194) of Spilka, Donnelly, Eldridge and other members of the General Court for legislation relative to the Commonwealth Fusion Center and other intelligence data centers [Joint Committee on Public Safety and Homeland Security].

[SIMILAR MATTER FILED IN PREVIOUS SESSION
SEE SENATE, NO. *931* OF 2009-2010.]

The Commonwealth of Massachusetts

In the Year Two Thousand Eleven

An Act to protect privacy and personal data.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. Section 18 of chapter 6A of the General Laws, as appearing in the 2008 Official Edition, is hereby amended by inserting after the word “board”, at line 5, the following:- - ; criminal intelligence systems operating in Massachusetts

SECTION 2. Section 18 ¾ of said chapter 6A, as so appearing, is hereby amended by adding at the end thereof:--

(10) to promulgate rules and regulations to ensure that criminal intelligence systems operating in Massachusetts, including but not limited to the commonwealth fusion center and the Boston regional intelligence center, as defined in chapter 66A of the General Laws:

(a) maintain records regarding the sources of criminal intelligence information and personal data, as defined in said Chapter 66A, that such criminal intelligence systems review, collect, and maintain, and the quantity of data received from each source;

(b) maintain criminal intelligence information or personal data concerning an individual or organization only if there is a reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity. Such reasonable suspicion is established when information exists which 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;

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

(c) disseminate criminal intelligence information or personal data only to law enforcement authorities which shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with the receipt, maintenance, security and dissemination limitations, requirements and procedures applicable to the criminal intelligence system. Nothing herein shall limit the dissemination of an assessment of intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property;

(d) notify submitting criminal justice agencies, law enforcement agencies, criminal intelligence systems or other submitting individuals prior to initiation of formal information exchange arrangements with any Federal, State, regional, or other information systems;

(e) adopt, implement, and maintain procedures to ensure the maximum feasible security, confidentiality, and integrity of personal information, as defined in Chapter 93H, and personal data, as defined in Chapter 66A, including but not limited to labeling all such data to indicate levels of sensitivity, levels of confidence, and the identity of the submitting criminal justice agency, law enforcement agency, or other submitting entity or individual;

(f) adopt, implement, and maintain written information security programs governing the collection, use, dissemination, storage, retention and destruction of personal information, as defined in Chapter 93H, and personal data, as defined in Chapter 66A, and ensure that criminal intelligence systems securely store and protect the information against unauthorized access, destruction, use, modification, disclosure or loss, and destroy the information as soon as it is no longer needed. Such programs shall address, without limitation, administrative, technical and physical safeguards, and shall include sanctions for unauthorized access, utilization, or disclosure of information stored and maintained by criminal intelligence systems, and shall comply with all federal and state privacy and information security laws and regulations, including but not limited to all applicable rules and regulations used by the Secretary of State's Supervisor of Public Records under Chapter 93H.

(g) file annually, on or before the first of September, a notice as directed by section sixty-three of Chapter 30.

(h) protect the security and privacy of data collected by criminal intelligence systems operating in Massachusetts by requiring that such criminal intelligence systems, at a minimum:

(i) address any participation by entities other than public law enforcement agencies in criminal intelligence system activities;

(ii) require any agency submitting data to a criminal intelligence system to maintain in its agency files documentation of each such submission, which shall be made available for reasonable audit and inspection by the inspector general;

(iii) establish protocols for screening, hiring, transferring, promoting, and terminating personnel authorized to have direct access to criminal intelligence information or personal data; and

(iv) implement subsection (10) of this section, as well as the provisions of Chapter 66A and section 1A of Chapter 276.

11) provide assistance and unrestricted access to the inspector general in the preparation of an annual report on the compliance of criminal intelligence systems with subsection (10), which report shall include recommendations for corrective action. Said report shall be filed annually on or before the thirtieth of April with the clerks' offices of the senate and the house of representatives, the ways and means committees of the senate and house of representatives, and the joint committee on state administration and regulatory oversight, which shall convene a public hearing concerning the report within 60 days of its filing.

SECTION 3. Section 63 of Chapter 30 of the General Laws, as appearing in the 2008 Official Edition, is hereby amended by striking the word "and", at line 19, and by inserting after

the word “system”, at line 21, the following:-- ; and (j) a signed certification by the individual identified herein at subsection (i) that acknowledges his or her personal accountability for the data maintained by and disseminated from the system and that the operations of the system are, to the best of his or her knowledge, in compliance with all applicable federal, state and local laws, ordinances, and regulations.

SECTION 4. Section 1 of Chapter 66A of the General Laws, as appearing in the 2008 Official Edition, is hereby amended by inserting the following definitions:--

“Boston Regional Intelligence Center”, that entity within the office of the police commissioner of the Boston police department responsible for collecting and analyzing criminal intelligence information within the Metro-Boston homeland security region, or any successor entity.

“Commonwealth Fusion Center”, that entity established by Executive Order 476 within the executive office of public safety and homeland security, or any successor entity.

“Criminal intelligence information”, data which has been evaluated to determine that it is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity.

“Criminal intelligence system”, the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information, including the commonwealth fusion center and the Boston regional intelligence center.

SECTION 5. Said section 1 of Chapter 66A, as so appearing, is hereby further amended by striking the words “such information is not contained in a public record, as defined in clause Twenty-sixth of section seven of chapter four and shall not include intelligence information, evaluative information or criminal offender record information as defined in section one hundred and sixty-seven of chapter six.”, at lines 34 through 39, and inserting in their place the following:-- personal data shall not include information that would reasonably be expected to: interfere with an ongoing criminal investigation or other law enforcement proceeding; constitute a clearly unwarranted invasion of personal privacy; disclose the identity of a confidential source; or endanger the life or physical safety of any individual.

SECTION 6. Said Chapter 66A is hereby amended by inserting after section 2 the following section:-

Section 2 ½. At least once annually, every criminal intelligence system shall conduct an internal audit, the results of which shall be public records. This audit shall include:

(1) For each database that contains personal data, the number of authorized users, each user’s level of access, and the quantity of data accessed by each user on a weekly basis;

(2) For each database that contains personal data, the number of transactions performed by transaction type, unique user, and access location;

(3) For each database that contains personal data, the quantity of data collected and maintained from each unique source, and the frequency of data from each source being used in an investigation;

(4) Since the last audit, the numbers of investigations authorized and denied under subsection (b)(4) of section 1A of Chapter 276;

(5) The number of investigations authorized under said subsection (b)(4) that remain open;

(6) For each open investigation authorized under said subsection (b)(4), the length of time the investigation has remained open and a justification for continued collection or maintenance of protected information;

(7) Since the last audit, the number of investigations authorized under said subsection (b)(4) that have led to indictments or prosecutions, and the names and docket numbers of resulting court proceedings;

(8) Since the last audit, the number of authorized disseminations under subsection (b)(3) of section 1A of Chapter 276, and to which entity each dissemination was made.

SECTION 7. Section 3 of said Chapter 66A, as so appearing, is hereby amended by inserting after the word “towns.”, at line 9, the following:- The Secretary of Public Safety and Security shall promulgate rules and regulations to carry out the purposes of this chapter which shall be applicable to the Commonwealth Fusion Center and other criminal intelligence systems, including those operated by public safety entities of the cities and towns.

SECTION 8. Chapter 276 of the General Laws is hereby amended by striking out section 1A, as appearing in the 2008 Official Edition, and inserting in place thereof the following section:-

Section 1A. (a) No state or local law enforcement agency, prosecutorial office, criminal intelligence system, police or peace officer, or agent thereof shall track, collect or maintain information about the political, religious or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership or other entity unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is involved in criminal conduct. Any information collected or maintained under this section shall be referred to hereinafter as "protected information."

(b) No criminal intelligence system, as defined in chapter 66A of the General Laws, or state or local law enforcement agency in receipt of information from an criminal intelligence system, shall collect, maintain, or disseminate protected information except in accordance with the provisions of this section:

(1) No protected information shall be knowingly received, maintained, or disseminated that has been obtained in violation of any applicable federal, state, or local law, ordinance, or regulation.

(2) All protected information shall be evaluated for the reliability of its source and the accuracy of its content prior to being recorded in any investigation file.

(3) Protected information shall be disseminated only to law enforcement agencies, contingent upon review and prior written authorization by the head of the originating law enforcement agency or criminal intelligence system. A record of any such written authorization, which shall specify the reasons the dissemination is necessary, shall be maintained for a minimum of five years. The originating entity shall record each instance of dissemination in a

log containing the name of the subject or subjects, the name of the entity with whom the information was shared, and the date of dissemination.

(4) All investigations undertaken on the basis of any protected information shall first be authorized in writing by the head of the investigating law enforcement agency or criminal intelligence system. A record of any such written authorization, which shall specify the reasons for such investigation, shall be maintained in the corresponding investigation file for a minimum of five years

(5) All information recorded in any investigation file shall be reviewed at least once every five years, and any information that is not reliable, accurate, relevant, and timely, shall be destroyed, provided however, that any documents related to the authorization for and termination of investigations based in whole or in part on protected information collected under section 1A of this chapter, and any authorization to disseminate such protected information, shall be retained. Information retained in an investigation file after a review shall be accompanied by the following documentation: the name of the reviewer, the date of review, and an explanation of the decision to retain the information.