SENATE DOCKET, NO. 132 FILED ON: 1/11/2013

SENATE . . . . . No. 642

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 passage of the accompanying:

An Act to protect freedom of speech and association.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
Harriette L. Chandler	*First Worcester*
Jason M. Lewis	*31st Middlesex*
William N. Brownsberger	*Second Suffolk and Middlesex*
James J. O'Day	*14th Worcester*
Gale D. Candaras	*First Hampden and Hampshire*
Sal N. DiDomenico	*Middlesex and Suffolk*
Kay Khan	*11th Middlesex*
Ryan C. Fattman	*18th Worcester*
Timothy J. Toomey, Jr.	*26th Middlesex*
Brian R. Mannal	*2nd Barnstable*
Michael Barrett	*Third Middlesex*
Patricia D. Jehlen	*Second Middlesex*
Michael O. Moore	*Second Worcester*
Mary S. Keefe	*15th Worcester*
Denise Andrews	*2nd Franklin*
Denise Provost	*27th Middlesex*
Harold P. Naughton, Jr.	*12th Worcester*
Thomas P. Conroy	*13th Middlesex*

Diana DiZoglio	*14th Essex*
Martha M. Walz	*8th Suffolk*

SENATE DOCKET, NO. 132 FILED ON: 1/11/2013

SENATE . . . . . No. 642

By Ms. Chandler, a petition (accompanied by bill, Senate, No. 642) of Harriette L. Chandler, Jason M. Lewis, William N. Brownsberger, James J. O'Day and other members of the General Court for legislation relative to freedom of speech and association. The Judiciary.

The Commonwealth of Massachusetts

An Act to protect freedom of speech and association.

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 1 of Chapter 66A of the General Laws, as appearing in the 2010 Official Edition, is hereby amended by striking out the definition of "Personal data", at lines 32 through 39, and inserting the following definitions:--

"Commonwealth Fusion Center", that entity established by Executive Order 476 within the executive office of public safety and 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. 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.

"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, the Boston regional intelligence center, and any successor entities.

"Personal data", any information concerning an individual which, because of name, identifying number, mark or description can be readily associated with a particular individual; provided, however, that 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.

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

25 Section 2 ½. At least once annually, every criminal intelligence system shall conduct an
26 internal audit, the report of which shall be a public record. This audit shall include:

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

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

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

34 (4) The numbers of investigations authorized and denied under subsection (b)(4) of
35 section 1A of Chapter 276;

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

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

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

44 (8) The number of authorized disseminations under subsection (b)(3) of section 1A of
45 Chapter 276, and to which entity each dissemination was made.

46 Section 2 ¾. Every criminal intelligence system shall provide assistance and unrestricted
47 access to the inspector general, who may from time to time prepare a report on the compliance of
48 criminal intelligence systems with section 1A of Chapter 276, which report shall include
49 recommendations for corrective action and be a public record.

50 SECTION 3. Chapter 276 of the General Laws is hereby amended by striking out section
51 1A and inserting in place thereof the following section:-

52 Section 1A. (a) No state or local law enforcement agency, prosecutorial office,
53 criminal intelligence system, police or peace officer, or agent thereof shall track, collect or
54 maintain information about the political, religious or social views, associations or activities of
55 any individual, group, association, organization, corporation, business or partnership or other

56 entity unless such information directly relates to an investigation of criminal activities, and there
57 are reasonable grounds to suspect the subject of the information is involved in criminal conduct.
58 Any information collected or maintained under this section shall be referred to hereinafter as
59 "protected information."

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

64 (1) No protected information obtained in violation of any applicable federal, state, or
65 local law, ordinance, or regulation shall be knowingly accessed, received, maintained, or
66 disseminated.

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

69 (3) Protected information shall be disseminated only to law enforcement agencies,
70 contingent upon review and prior written authorization by the head of the originating law
71 enforcement agency or criminal intelligence system. A record of any such written authorization,
72 which shall specify the reasons the dissemination is necessary, shall be maintained for a
73 minimum of five years. The originating entity shall record each instance of dissemination,
74 whether written or oral, in a log containing the name of the subject or subjects, the name of the
75 entity with whom the information was shared, and the date of dissemination.

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

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