

HOUSE No. 1336

The Commonwealth of Massachusetts

PRESENTED BY:

Jason M. Lewis

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 Privacy and Personal Data.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
<i>Kevin J. Kuros</i>	<i>8th Worcester</i>
<i>Jason M. Lewis</i>	<i>31st Middlesex</i>
<i>Frank I. Smizik</i>	<i>15th Norfolk</i>
<i>William N. Brownsberger</i>	<input type="checkbox"/> [District] <input type="checkbox"/>
<i>Peter V. Kocot</i>	<i>1st Hampshire</i>
<i>John P. Fresolo</i>	<i>16th Worcester</i>
<i>Kay Khan</i>	<i>11th Middlesex</i>
<i>Denise Andrews</i>	<i>2nd Franklin</i>
<i>James Arciero</i>	<i>2nd Middlesex</i>
<i>Cory Atkins</i>	<i>14th Middlesex</i>
<i>Ruth B. Balsler</i>	<i>12th Middlesex</i>
<i>Jennifer E. Benson</i>	<i>37th Middlesex</i>
<i>Linda Campbell</i>	<i>15th Essex</i>
<i>Gailanne M. Cariddi</i>	<i>1st Berkshire</i>
<i>Thomas P. Conroy</i>	<i>13th Middlesex</i>
<i>Carolyn C. Dykema</i>	<i>8th Middlesex</i>

James B. Eldridge

-
-

[District]

Christopher G. Fallon

33rd Middlesex

Linda Dorcena Forry

12th Suffolk

Sean Garballey

23rd Middlesex

Jonathan Hecht

29th Middlesex

Bradley H. Jones, Jr.

20th Middlesex

Jay R. Kaufman

15th Middlesex

Stephen Kulik

1st Franklin

Steven L. Levy

4th Middlesex

Elizabeth A. Malia

11th Suffolk

James J. O'Day

14th Worcester

George N. Peterson, Jr.

9th Worcester

Byron Rushing

9th Suffolk

Jeffrey Sánchez

15th Suffolk

John W. Scibak

2nd Hampshire

Carl M. Sciortino, Jr.

34th Middlesex

Theodore C. Speliotis

13th Essex

William M. Straus

10th Bristol

Benjamin Swan

11th Hampden

Chris Walsh

6th Middlesex

Martha M. Walz

8th Suffolk

Thomas M. Petrolati

7th Hampden

Paul Adams

17th Essex

HOUSE No. 1336

By Mr. Lewis of Winchester, a petition (accompanied by bill, House, No. 1336) of Jason M. Lewis and others for legislation to regulate the collection and maintenance of criminal intelligence information. The Judiciary.

The Commonwealth of Massachusetts

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:

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

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

6 ; criminal intelligence systems operating in Massachusetts

7 SECTION 2. Section 18 ³/₄ of said chapter 6A, as so appearing, is hereby amended by
8 adding at the end thereof:--

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

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

15 (b) maintain criminal intelligence information or personal data concerning an individual
16 or organization only if there is a reasonable suspicion that the individual is involved in criminal
17 conduct or activity and the information is relevant to that criminal conduct or activity. Such
18 reasonable suspicion is established when information exists which establishes sufficient facts to
19 give a trained law enforcement or criminal justice agency officer, investigator, or employee a
20 basis to believe that there is a reasonable possibility that an individual or organization is involved
21 in a definable criminal activity or enterprise;

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

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

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

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

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

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

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

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

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

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

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

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

72

73 SECTION 3. Section 63 of Chapter 30 of the General Laws, as appearing in the 2008
74 Official Edition, is hereby amended by striking the word "and", at line 19, and by inserting after
75 the word "system", at line 21, the following:-- ; and (j) a signed certification by the individual
76 identified herein at subsection (i) that acknowledges his or her personal accountability for the
77 data maintained by and disseminated from the system and that the operations of the system are,
78 to the best of his or her knowledge, in compliance with all applicable federal, state and local
79 laws, ordinances, and regulations.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

127 SECTION 7. Section 3 of said Chapter 66A, as so appearing, is hereby amended by
128 inserting after the word “towns.”, at line 9, the following:-

129 The Secretary of Public Safety and Security shall promulgate rules and regulations to
130 carry out the purposes of this chapter which shall be applicable to the Commonwealth Fusion
131 Center and other criminal intelligence systems, including those operated by public safety entities
132 of the cities and towns.

133 SECTION 8. Chapter 276 of the General Laws is hereby amended by striking out section
134 1A, as appearing in the 2008 Official Edition, and inserting in place thereof the following
135 section:-

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

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

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

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

153 (3) Protected information shall be disseminated only to law enforcement agencies,
154 contingent upon review and prior written authorization by the head of the originating law
155 enforcement agency or criminal intelligence system. A record of any such written authorization,
156 which shall specify the reasons the dissemination is necessary, shall be maintained for a
157 minimum of five years. The originating entity shall record each instance of dissemination in a
158 log containing the name of the subject or subjects, the name of the entity with whom the
159 information was shared, and the date of dissemination.

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

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