

HOUSE No. 01336

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 bill:

An Act to Protect Privacy and Personal Data.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
<i>Frank I. Smizik</i>	<i>15th Norfolk</i>
<i>William N. Brownsberger</i>	<i>24th Middlesex</i>
<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. Balse</i>	<i>12th Middlesex</i>
<i>Jennifer E. Benson</i>	<i>37th Middlesex</i>
<i>Linda Dean Campbell</i>	<i>15th Essex</i>
<i>Gailanne Cariddi</i>	<i>1st Berkshire</i>
<i>Thomas P. Conroy</i>	<i>13th Middlesex</i>
<i>Carolyn C. Dykema</i>	<i>8th Middlesex</i>
<i>James B. Eldridge</i>	<i>Middlesex and Worcester</i>
<i>Christopher G. Fallon</i>	<i>33rd Middlesex</i>
<i>Linda Dorcena Forry</i>	<i>12th Suffolk</i>

<i>Sean Garballey</i>	<i>23rd Middlesex</i>
<i>Jonathan Hecht</i>	<i>29th Middlesex</i>
<i>Bradley H. Jones, Jr.</i>	<i>20th Middlesex</i>
<i>Jay Kaufman</i>	<i>15th Middlesex</i>
<i>Stephen Kulik</i>	<i>1st Franklin</i>
<i>Steven L. Levy</i>	<i>4th Middlesex</i>
<i>Elizabeth A. Malia</i>	<i>11th Suffolk</i>
<i>James J. O'Day</i>	<i>14th Worcester</i>
<i>George N. Peterson, Jr.</i>	<i>9th Worcester</i>
<i>Byron Rushing</i>	<i>9th Suffolk</i>
<i>Jeffrey Sánchez</i>	<i>15th Suffolk</i>
<i>John W. Scibak</i>	<i>2nd Hampshire</i>
<i>Carl M. Sciortino, Jr.</i>	<i>34th Middlesex</i>
<i>Theodore C. Speliotis</i>	<i>13th Essex</i>
<i>William M. Straus</i>	<i>10th Bristol</i>
<i>Benjamin Swan</i>	<i>11th Hampden</i>
<i>Chris Walsh</i>	<i>6th Middlesex</i>
<i>Martha M. Walz</i>	<i>8th Suffolk</i>
<i>Thomas M. Petrolati</i>	<i>7th Hampden</i>
<i>Paul Adams</i>	<i>17th Essex</i>
<i>Alice K. Wolf</i>	<i>25th Middlesex</i>

HOUSE No. 01336

By Mr. Jason M. Lewis of Winchester, petition (accompanied by bill, House, No. 01336) of Alice K. Wolf and others for legislation to regulate the collection and maintenance of criminal intelligence information. Joint Committee on the Judiciary.

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:

1 Be it enacted by the Senate and House of Representatives in General Court assembled,
2 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 Official
4 Edition, is hereby amended by inserting after the word “board”, at line 5, the following:--

5 ; criminal intelligence systems operating in Massachusetts

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

8 (10) to promulgate rules and regulations to ensure that criminal intelligence systems operating in
9 Massachusetts, including but not limited to the commonwealth fusion center and the Boston

10 regional intelligence center, as defined in chapter 66A of the General Laws:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

69

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

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

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

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

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

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

91 SECTION 5. Said section 1 of Chapter 66A, as so appearing, is hereby further amended by
92 striking the words “such information is not contained in a public record, as defined in clause
93 Twenty-sixth of section seven of chapter four and shall not include intelligence information,
94 evaluative information or criminal offender record information as defined in section one hundred
95 and sixty-seven of chapter six.”, at lines 34 through 39, and inserting in their place the
96 following:-- personal data shall not include information that would reasonably be expected to:
97 interfere with an ongoing criminal investigation or other law enforcement proceeding; constitute

98 a clearly unwarranted invasion of personal privacy; disclose the identity of a confidential source;
99 or endanger the life or physical safety of any individual.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

158 (5) All information recorded in any investigation file shall be reviewed at least once every five
159 years, and any information that is not reliable, accurate, relevant, and timely, shall be destroyed,

160 provided however, that any documents related to the authorization for and termination of
161 investigations based in whole or in part on protected information collected under section 1A of
162 this chapter, and any authorization to disseminate such protected information, shall be retained.
163 Information retained in an investigation file after a review shall be accompanied by the following
164 documentation: the name of the reviewer, the date of review, and an explanation of the decision
165 to retain the information.