

HOUSE No. 2332

The Commonwealth of Massachusetts

PRESENTED BY:

Sarah K. Peake

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 electronic privacy.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
<i>Sarah K. Peake</i>	<i>4th Barnstable</i>
<i>Adrian Madaro</i>	<i>1st Suffolk</i>
<i>José F. Tosado</i>	<i>9th Hampden</i>
<i>Timothy R. Whelan</i>	<i>1st Barnstable</i>
<i>Denise Provost</i>	<i>27th Middlesex</i>
<i>Frank A. Moran</i>	<i>17th Essex</i>
<i>Jay R. Kaufman</i>	<i>15th Middlesex</i>
<i>Sean Garballey</i>	<i>23rd Middlesex</i>
<i>Leonard Mirra</i>	<i>2nd Essex</i>
<i>William M. Straus</i>	<i>10th Bristol</i>
<i>David M. Rogers</i>	<i>24th Middlesex</i>
<i>Angelo J. Puppolo, Jr.</i>	<i>12th Hampden</i>
<i>John W. Scibak</i>	<i>2nd Hampshire</i>
<i>Josh S. Cutler</i>	<i>6th Plymouth</i>
<i>Steven S. Howitt</i>	<i>4th Bristol</i>
<i>Frank I. Smizik</i>	<i>15th Norfolk</i>
<i>Edward F. Coppinger</i>	<i>10th Suffolk</i>
<i>Tackey Chan</i>	<i>2nd Norfolk</i>

<i>Ruth B. Balsler</i>	<i>12th Middlesex</i>
<i>Thomas M. McGee</i>	<i>Third Essex</i>
<i>F. Jay Barrows</i>	<i>1st Bristol</i>
<i>William L. Crocker, Jr.</i>	<i>2nd Barnstable</i>
<i>John J. Lawn, Jr.</i>	<i>10th Middlesex</i>
<i>Barbara A. L'Italien</i>	<i>Second Essex and Middlesex</i>
<i>Carolyn C. Dykema</i>	<i>8th Middlesex</i>
<i>Thomas M. Stanley</i>	<i>9th Middlesex</i>
<i>Chris Walsh</i>	<i>6th Middlesex</i>
<i>Jack Lewis</i>	<i>7th Middlesex</i>
<i>Jennifer E. Benson</i>	<i>37th Middlesex</i>
<i>Mike Connolly</i>	<i>26th Middlesex</i>
<i>Ann-Margaret Ferrante</i>	<i>5th Essex</i>
<i>Kevin G. Honan</i>	<i>17th Suffolk</i>
<i>Kenneth I. Gordon</i>	<i>21st Middlesex</i>
<i>Dylan Fernandes</i>	<i>Barnstable, Dukes and Nantucket</i>
<i>Paul McMurtry</i>	<i>11th Norfolk</i>
<i>Kay Khan</i>	<i>11th Middlesex</i>
<i>Daniel M. Donahue</i>	<i>16th Worcester</i>
<i>Michael J. Moran</i>	<i>18th Suffolk</i>
<i>James M. Cantwell</i>	<i>4th Plymouth</i>
<i>Paul J. Donato</i>	<i>35th Middlesex</i>
<i>Carmine L. Gentile</i>	<i>13th Middlesex</i>
<i>Randy Hunt</i>	<i>5th Barnstable</i>
<i>Byron Rushing</i>	<i>9th Suffolk</i>
<i>Gailanne M. Cariddi</i>	<i>1st Berkshire</i>
<i>Marjorie C. Decker</i>	<i>25th Middlesex</i>
<i>Louis L. Kafka</i>	<i>8th Norfolk</i>
<i>Jason M. Lewis</i>	<i>Fifth Middlesex</i>
<i>Smitty Pignatelli</i>	<i>4th Berkshire</i>
<i>Paul R. Heroux</i>	<i>2nd Bristol</i>
<i>Jay D. Livingstone</i>	<i>8th Suffolk</i>
<i>Robert M. Koczera</i>	<i>11th Bristol</i>
<i>Jonathan Hecht</i>	<i>29th Middlesex</i>
<i>Bruce J. Ayers</i>	<i>1st Norfolk</i>
<i>Susan Williams Gifford</i>	<i>2nd Plymouth</i>
<i>Antonio F. D. Cabral</i>	<i>13th Bristol</i>
<i>Brian M. Ashe</i>	<i>2nd Hampden</i>
<i>Kevin J. Kuros</i>	<i>8th Worcester</i>

<i>Patrick M. O'Connor</i>	<i>Plymouth and Norfolk</i>
<i>Thomas J. Calter</i>	<i>12th Plymouth</i>
<i>Cory Atkins</i>	<i>14th Middlesex</i>
<i>Bradley H. Jones, Jr.</i>	<i>20th Middlesex</i>
<i>James J. Dwyer</i>	<i>30th Middlesex</i>
<i>Angelo L. D'Emilia</i>	<i>8th Plymouth</i>
<i>Danielle W. Gregoire</i>	<i>4th Middlesex</i>
<i>Angelo M. Scaccia</i>	<i>14th Suffolk</i>
<i>Aaron Vega</i>	<i>5th Hampden</i>
<i>James B. Eldridge</i>	<i>Middlesex and Worcester</i>
<i>Paul W. Mark</i>	<i>2nd Berkshire</i>
<i>Keiko M. Orrall</i>	<i>12th Bristol</i>
<i>Michelle M. DuBois</i>	<i>10th Plymouth</i>
<i>Jennifer L. Flanagan</i>	<i>Worcester and Middlesex</i>
<i>Hannah Kane</i>	<i>11th Worcester</i>
<i>John J. Mahoney</i>	<i>13th Worcester</i>
<i>Kate Hogan</i>	<i>3rd Middlesex</i>
<i>Joseph W. McGonagle, Jr.</i>	<i>28th Middlesex</i>
<i>Nicholas A. Boldyga</i>	<i>3rd Hampden</i>
<i>Joan B. Lovely</i>	<i>Second Essex</i>
<i>Evandro C. Carvalho</i>	<i>5th Suffolk</i>
<i>Harold P. Naughton, Jr.</i>	<i>12th Worcester</i>
<i>Peter V. Kocot</i>	<i>1st Hampshire</i>
<i>Christine P. Barber</i>	<i>34th Middlesex</i>
<i>Russell E. Holmes</i>	<i>6th Suffolk</i>
<i>Patricia A. Haddad</i>	<i>5th Bristol</i>
<i>Aaron Michlewitz</i>	<i>3rd Suffolk</i>
<i>Ryan C. Fattman</i>	<i>Worcester and Norfolk</i>
<i>Brendan P. Crighton</i>	<i>Third Essex</i>
<i>Daniel J. Hunt</i>	<i>13th Suffolk</i>
<i>Michael S. Day</i>	<i>31st Middlesex</i>
<i>Claire D. Cronin</i>	<i>11th Plymouth</i>
<i>Steven Ultrino</i>	<i>33rd Middlesex</i>
<i>Jonathan D. Zlotnik</i>	<i>2nd Worcester</i>
<i>Linda Dorcena Forry</i>	<i>First Suffolk</i>
<i>David T. Vieira</i>	<i>3rd Barnstable</i>
<i>Daniel J. Ryan</i>	<i>2nd Suffolk</i>
<i>Michael O. Moore</i>	<i>Second Worcester</i>
<i>Brian Murray</i>	<i>10th Worcester</i>

<i>Bruce E. Tarr</i>	<i>First Essex and Middlesex</i>
<i>Marc R. Pacheco</i>	<i>First Plymouth and Bristol</i>
<i>Alice Hanlon Peisch</i>	<i>14th Norfolk</i>
<i>Stephan Hay</i>	<i>3rd Worcester</i>
<i>Paul Brodeur</i>	<i>32nd Middlesex</i>

HOUSE No. 2332

By Ms. Peake of Provincetown, a petition (accompanied by bill, House, No. 2332) of Sarah K. Peake and others for legislation to update penalties and protect electronic privacy. The Judiciary.

The Commonwealth of Massachusetts

**In the One Hundred and Ninetieth General Court
(2017-2018)**

An Act to protect electronic privacy.

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

1 SECTION 1. Chapter 276 of the General Laws, as appearing in the 2014 official edition,
2 is hereby amended by striking Section 1B and inserting in its place the following:-

3 Section 1B. (a) As used in this section, the following words shall have the following
4 meanings:

5 "Adverse result", occurs when notification of the existence of a search warrant results in:

6 (1) danger to the life or physical safety of an individual;

7 (2) a flight from prosecution;

8 (3) the destruction of or tampering with evidence;

9 (4) the intimidation of a potential witness or witnesses; or

10 (5) serious jeopardy to an investigation or undue delay of a trial.

11 "Cell site simulator device", a device that transmits or receives radio waves to simulate an
12 electronic device, cell tower, cell site, or service for the purpose of conducting one or more of the
13 following operations: (i) identifying, locating, or tracking the movements of an electronic device;
14 (ii) intercepting, obtaining, accessing, or forwarding the communications, stored data, or
15 metadata of an electronic device; (iii) affecting the hardware or software operations or functions
16 of an electronic device; (iv) forcing transmissions from or connections to an electronic device; or
17 (v) denying an electronic device access to other electronic devices, communications protocols, or
18 services.

19 "Electronic communication services", shall be construed in accordance with sections
20 2701 to 2711 Title 18, of the United States Code. This definition shall not apply to corporations
21 that do not provide electronic communication services to the general public.

22 "Electronic device", any device that enables access to, or use of, an electronic
23 communication service, remote computing service or location information service.

24 "Foreign corporation", any corporation or other entity that makes a contract or engages in
25 a terms of service agreement with a resident of the commonwealth to be performed in whole or
26 in part by either party in the commonwealth. The making of the contract or terms of service
27 agreement shall be considered to be the agreement of the foreign corporation that a search
28 warrant or subpoena which has been properly served on it has the same legal force and effect as
29 if served personally within the commonwealth.

30 "Location information", any information concerning the location of an electronic device
31 that, in whole or in part, is generated by or derived from the device or any of its applications.

32 “Location information service”, a global positioning service or other mapping, locational
33 or directional information service.

34 "Massachusetts corporation", any corporation or other entity that is subject to chapter 155
35 or chapter 156B.

36 “Metadata”, information, other than communications content, which is necessary to or
37 associated with the provision of electronic communication services, remote computing services,
38 or location information services, including but not limited to information about the source or
39 destination of electronic communications, date and time of electronic communications, delivery
40 instructions, account information, internet protocol address, quantum of data, data or file type, or
41 data tags.

42 "Properly served", delivery of a search warrant or subpoena by hand, by United States
43 mail, by commercial delivery service, by facsimile or by any other manner to any officer of a
44 corporation or its general manager in the commonwealth, to any natural person designated by it
45 as agent for the service of process, or if such corporation has designated a corporate agent, to any
46 person named in the latest certificate filed pursuant to section 15.03 of chapter 156D.

47 "Remote computing services", shall be construed in accordance with sections 2701 to
48 2711, inclusive, of Title 18, of the United States Code. This definition shall not apply to
49 corporations that do not provide those services to the general public.

50 "Subpoena", a grand jury or trial subpoena issued in the course of a criminal proceeding
51 or an administrative subpoena issued pursuant to section 17B of chapter 271.

52 (b) A government office or public official may obtain or access the following information
53 only (1) with a person's informed consent, (2) pursuant to a warrant issued by a judicial officer
54 upon an application demonstrating probable cause, or (3) acting in accordance with a legally
55 recognized exception to the warrant requirement:

56 (i) data stored by or on behalf of a user of those services;

57 (ii) any content of communications transmitted by an electronic device or stored by those
58 services; or

59 (iii) location information.

60 (c) A government office or public official may use a cell site simulator device to obtain or
61 access information, including metadata, only (1) with the informed consent of the user of the
62 targeted electronic device, (2) pursuant to a probable cause warrant issued upon an application
63 specifically stating that use of a cell site simulator is sought, or (3) acting in accordance with a
64 legally recognized exception to the warrant requirement.

65 (d) Upon complaint on oath that the complainant believes that (1) particular identified
66 records or information are in the actual or constructive custody of a Massachusetts or foreign
67 corporation providing electronic communication services, remote computing services, or location
68 information services, and (2) such records or information constitute evidence of or the means or
69 instrumentalities of the commission of a specified criminal offense under the laws of the
70 commonwealth, a justice of the superior court may, if satisfied that there is probable cause for
71 such beliefs, issue a warrant identifying those records to be sought and authorizing the person
72 making application for the warrant to properly serve the warrant upon the corporation and to take
73 all other actions prescribed by this section.

74 (e) Upon complaint on oath that the complainant believes that the use of a cell site
75 simulator device will lead to (i) evidence of or the means or instrumentalities of the commission
76 of a specified criminal offense under the laws of the commonwealth or (ii) the location of a
77 person whom there is probable cause to believe has committed, is committing, or is about to
78 commit a crime, a justice of the superior court may, if satisfied that probable cause has been
79 established for such belief, issue a warrant authorizing that particular information be sought from
80 a specified electronic device or, if the complainant is unable to specify the particular device,
81 from electronic devices at a specified location, stating the duration for authorized use of the cell
82 site simulator device, and directing the person authorized by the warrant to take all other actions
83 prescribed by this section.

84 A warrant application to use a cell site simulator device shall: (i) specify sufficient facts
85 to demonstrate that alternative methods of investigation and surveillance with less incidental
86 impact on non-targeted parties and electronic devices are inadequate to achieve the same
87 purposes; and (ii) identify the law enforcement agency that owns the cell site simulator device, if
88 different from the law enforcement agency making the application.

89 If the application seeks authority to use a cell site simulator device to intercept the
90 contents of oral communications, authorization may be granted only in compliance with the
91 procedural and substantive requirements contained in section 99 of chapter 272 and federal law
92 concerning wiretaps.

93 (f) Search warrants issued under this section shall designate the person, corporation or
94 other entity, if any, in possession of the records or data sought, and shall describe, with
95 particularity, the information sought and to be provided. They shall be issued in the form and

96 manner prescribed in sections 2A½ and 2B, insofar as they are applicable, and shall be directed
97 to the law enforcement officer or government office making application for the warrant.

98 (g) The following provisions shall apply to any search warrant issued under this section
99 and to any subpoena issued in the course of a criminal investigation or proceeding directed to a
100 Massachusetts or foreign corporation that provides electronic communication services, remote
101 computing services or location information services:

102 (1) when properly served with a search warrant issued by any court of the commonwealth
103 or justice pursuant to this section or a subpoena, a corporation subject to this section shall
104 provide all records sought pursuant to that warrant or subpoena within 14 days of receipt,
105 including those records maintained or located outside the commonwealth;

106 (2) if the applicant makes a showing and the court or justice finds that failure to produce
107 records within less than 14 days would cause an adverse result, a warrant may require production
108 of records within less than 14 days;

109 (3) a court or justice may reasonably extend the time required for production of the
110 records upon finding that the corporation has shown good cause for that extension and that an
111 extension of time would not cause an adverse result;

112 (4) a corporation seeking to quash a warrant or subpoena served on it pursuant to this
113 section shall seek relief from the court that issued the warrant or the court which has jurisdiction
114 over the subpoena within the time required for production of records pursuant to this section. The
115 court shall hear and decide such motion not later than 14 days after the motion is filed;

116 (5) in the case of an administrative subpoena issued by the attorney general, the superior
117 court of Suffolk county shall have jurisdiction and in the case of an administrative subpoena
118 issued by a district attorney, the superior court in any county in which the district attorney
119 maintains an office shall have jurisdiction; and

120 (6) the corporation shall verify the authenticity of records that it produces by providing an
121 affidavit from the person in custody of those records certifying that they are true and complete.

122 (h) A Massachusetts corporation that provides electronic communication services or
123 remote computing services, when served with a warrant or subpoena issued by another state to
124 produce records that would reveal the identity of the customers using those services, data stored
125 by, or on behalf of the customer, the customer's usage of those services, the recipient or
126 destination of communications sent to or from those customers, or the content of those
127 communications, shall produce those records as if that warrant or subpoena had been issued
128 under the law of the commonwealth.

129 (i) No cause of action shall lie against any foreign or Massachusetts corporation subject
130 to this section, its officers, employees, agents or other persons for providing records,
131 information, facilities or assistance in accordance with the terms of a warrant or subpoena issued
132 pursuant to this section.

133 (j) A law enforcement officer or agency authorized to use a cell site simulator device in
134 accordance with this section shall: (i) take all steps necessary to limit the collection of any
135 information or metadata to the target specified in the application and warrant authorization; (ii)
136 take all steps necessary to permanently delete any information or metadata collected from any
137 person or persons not specified in the warrant immediately following such collection and ensure

138 that such information or metadata is not used, retained, or transmitted for any purpose
139 whatsoever; and (iii) delete any information or metadata collected from the person or persons
140 specified in the warrant authorization within thirty days if there is no longer probable cause to
141 support the belief that such information or metadata is evidence of a crime.

142 (k) Not later than 7 days after information is obtained by a law enforcement officer or
143 government office pursuant to a warrant under this section, that officer or office shall serve upon,
144 or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated
145 to be effective as specified by the court issuing the warrant, to the customer or subscriber, or user
146 of an electronic device targeted by a cell site simulator device, a copy of the warrant, a copy of
147 the application for the warrant and notice that informs the customer, subscriber, or user of the
148 following:

149 (1) the nature of the law enforcement inquiry with reasonable specificity;

150 (2) in the case of information maintained for the customer or subscriber by the
151 provider of an electronic communications service, remote computing service or location
152 information service, that such information was requested by or supplied to that government
153 office or public official, a description of that information, and the dates on which the request was
154 made and on which the information was supplied;

155 (3) in the case of information obtained or accessed by means of a cell site simulator
156 device, a description of that information, and the dates, times, durations, and locations of the
157 search;

158 (4) whether notification of the customer, subscriber, or user was delayed under
159 subsection (j); and

160 (5) which court made the certification or determination under which that delay was
161 made, if applicable.

162 (l) A government office or public official may include in its application for a warrant a
163 request for an order delaying the notification required under subsection (k) for a period not to
164 exceed 90 days, and the court may issue the order if it determines there is reason to believe that
165 notification of the existence of the warrant may have an adverse result. Upon expiration of any
166 period of delay granted under this subsection, the government office or public official shall
167 provide the customer or subscriber a copy of the warrant together with notice required under, and
168 by the means described in, subsection (k).

169 A government office or public official may include in its application for a warrant a
170 request for an order directing a corporation or other entity to which a warrant is directed not to
171 notify any other person of the existence of the warrant for a period of not more than 90 days, and
172 the court may issue the order if the court determines that there is reason to believe that
173 notification of the existence of the warrant will have an adverse result.

174 The court may, upon application, grant 1 or more extensions of orders delaying
175 notification for an additional 90 days if the court determines that there is reason to believe that
176 notification of the existence of the warrant will have an adverse result.

177 (m) Notwithstanding any general or special law to the contrary, a government office or
178 public official may obtain information described in subsections (b) or (c):

179 (1) with the specific contemporaneous consent of the owner or user of the electronic
180 communications device concerned;

181 (2) in order to respond to the user's call for emergency services; or

182 (3) if it reasonably believes that an emergency involving immediate danger of death
183 or serious physical injury to any person requires obtaining without delay information relating to
184 the emergency; provided, however, that the request is narrowly tailored to address the emergency
185 and subject to the following limitations:

186 (i) the request shall document the factual basis for believing that an emergency
187 involving immediate danger of death or serious physical injury to a person requires obtaining
188 without delay of the information relating to the emergency; and

189 (ii) not later than 48 hours after the government office obtains access to records, it
190 shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank
191 designated by the head of the office setting forth the grounds for the emergency access.

192 (n) On the second Friday of January of each calendar year, any judge issuing or denying a
193 warrant under this section during the preceding calendar year shall report on each such warrant
194 to the office of court management within the trial court:

195 (1) the name of the agency making the application;

196 (2) the offense specified in the warrant or application therefor;

197 (3) the nature of the information sought;

198 (4) if the warrant application sought authorization to obtain or access information by
199 means of a cell site simulator device;

- 200 (5) if the warrant application sought authorization to obtain or access information
201 from a corporation or other entity, the name of that entity;
- 202 (6) whether the warrant was granted as applied for, was modified or was denied;
- 203 (7) the period of disclosures or access authorized by the warrant;
- 204 (8) the number and duration of any extensions of the warrant; and
- 205 (9) any order directing delayed notification of the warrant's existence.

206 In June of each year, the court administrator in the office of court management within the
207 trial court shall transmit to the legislature a full and complete report concerning the number of
208 applications for warrants authorizing or requiring the disclosure of or access to information
209 under this section. The reports shall include a summary and analysis of the data required to be
210 filed with that office. The reports shall be filed with the offices of the clerk of the house and the
211 senate and shall be public records. The court administrator in the office of court management
212 within the trial court shall issue guidance regarding the form of the reports.

213 (o) Except in a judicial proceeding alleging a violation of this section, no information
214 obtained in violation of this section and no information provided beyond the scope of the
215 materials authorized to be obtained shall be admissible in any criminal, civil, administrative or
216 other proceeding.

217 (p) The requirements of this section shall apply to all state and local law enforcement
218 officers operating in the commonwealth, whether said officers are assigned to state and local law
219 enforcement operations exclusively, or to joint task force or other collaborative operations with
220 federal law enforcement agencies.

221 SECTION 2. Chapter 276 is hereby amended by inserting after section 2A the following
222 section:-

223 Section 2A½. (a) A warrant issued pursuant to section 1B for records or data from a
224 corporation providing electronic communication services, remote computing services or location
225 information services shall be in substantially the following form:

226 THE COMMONWEALTH OF MASSACHUSETTS.

227 (COUNTY), ss. (NAME) COURT.

228 To the Sheriffs of our several counties, or their deputies, any State Police Officer, or a
229 Police Officer of any city or town in the Commonwealth.

230 Proof by affidavit having been made this day before (name and office of person
231 authorized to issue warrant) by (names of person or persons whose affidavits have been taken)
232 that there is probable cause for believing that certain records or data are in the in the possession
233 of (identify corporation or other entity) and that those records or data constitute evidence of or
234 the means or instrumentalities of the commission of (specified criminal offense under the laws of
235 the commonwealth).

236 We therefore authorize you to present this warrant to (identify corporation or other
237 entity), which warrant shall operate as an order for immediate disclosure of the following records
238 or data:

239 (description of particular records or data),

240 and if any such records or data are disclosed to bring it before (court having jurisdiction)
241 at (name of court and location).

242 Dated at (city or town) this _____ day of _____, (insert year).

243 Justice of the Superior Court

244 (b) A warrant issued pursuant to section 1B authorizing the use of a cell site simulator
245 device shall be in substantially the following form:

246 THE COMMONWEALTH OF MASSACHUSETTS.

247 (COUNTY), ss. (NAME) COURT.

248 To the Sheriff, or their deputy, State Police Officer, or municipal Police Officer who has
249 made this complaint on oath.

250 Proof by affidavit having been made this day before (name and office of person
251 authorized to issue warrant) by (names of person or persons whose affidavits have been taken)
252 that there is probable cause for believing that the use of a cell site simulator device will lead to
253 evidence of or the means or instrumentalities of the commission of (specified criminal offense
254 under the laws of the commonwealth) or the location of a person whom there is probable cause
255 to believe has committed, is committing, or is about to commit (specified criminal offense under
256 the laws of the commonwealth).

257 We therefore authorize you to obtain or access by means of a cell site simulator device,
258 the following records or data:

259 (description of particular records or data),

260 and if any such records or data are disclosed to bring it before (court having jurisdiction)
261 at (name of court and location).

262 Dated at (city or town) this _____ day of _____, (insert year).

263 Justice of the Superior Court

264

265 SECTION 3. Section 2B of said chapter 276, as appearing in the 2014 official edition, is
266 hereby amended by striking clauses 3 and 4 of the model affidavit and inserting in place thereof
267 the following:-

268 3. Based upon the foregoing reliable information (and upon my personal knowledge)
269 there is probable cause to believe that the property, records or data hereinafter described (has
270 been stolen, or is being concealed, or constitutes evidence of a particular offense, etc.) and may
271 be found (in the possession of A. B. or any other person or corporation) at premises (identify).

272 4. The (property, records, or data) for which I seek issuance of a search warrant is the
273 following: (here describe the property, records, or data as particularly as possible).