SENATE DOCKET, NO. 1175 FILED ON: 1/19/2017

SENATE . . . . . No. 943

The Commonwealth of Massachusetts

PRESENTED BY:

Karen E. Spilka

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:	
Karen E. Spilka	*Second Middlesex and Norfolk*	
Jay R. Kaufman	*15th Middlesex*	*1/24/2017*
Jason M. Lewis	*Fifth Middlesex*	*1/25/2017*
Thomas M. McGee	*Third Essex*	*1/25/2017*
F. Jay Barrows	*1st Bristol*	*1/25/2017*
Michael J. Barrett	*Third Middlesex*	*1/26/2017*
Jack Lewis	*7th Middlesex*	*1/27/2017*
Byron Rushing	*9th Suffolk*	*1/30/2017*
Marjorie C. Decker	*25th Middlesex*	*1/30/2017*
Donald F. Humason, Jr.	*Second Hampden and Hampshire*	*1/30/2017*
Kenneth J. Donnelly	*Fourth Middlesex*	*1/30/2017*
Kay Khan	*11th Middlesex*	*1/30/2017*
Sal N. DiDomenico	*Middlesex and Suffolk*	*1/31/2017*
Barbara A. L'Italien	*Second Essex and Middlesex*	*1/31/2017*
Patrick M. O'Connor	*Plymouth and Norfolk*	*1/31/2017*
Bradley H. Jones, Jr.	*20th Middlesex*	*1/31/2017*
Cynthia S. Creem	*First Middlesex and Norfolk*	*1/31/2017*
Kate Hogan	*3rd Middlesex*	*2/2/2017*

Joan B. Lovely	*Second Essex*	*2/2/2017*
William N. Brownsberger	*Second Suffolk and Middlesex*	*2/2/2017*
Keiko M. Orrall	*12th Bristol*	*2/2/2017*
Carolyn C. Dykema	*8th Middlesex*	*2/2/2017*
Anne M. Gobi	*Worcester, Hampden, Hampshire and Middlesex*	*2/2/2017*
Eric P. Lesser	*First Hampden and Hampshire*	*2/3/2017*
Linda Dorcena Forry	*First Suffolk*	*2/3/2017*
Jeffrey N. Roy	*10th Norfolk*	*2/3/2017*
Daniel J. Ryan	*2nd Suffolk*	*2/3/2017*
Michael O. Moore	*Second Worcester*	*2/3/2017*
Elizabeth A. Malia	*11th Suffolk*	*2/3/2017*
Marc R. Pacheco	*First Plymouth and Bristol*	*2/3/2017*
Mark C. Montigny	*Second Bristol and Plymouth*	*2/3/2017*
James B. Eldridge	*Middlesex and Worcester*	*2/3/2017*
Alice Hanlon Peisch	*14th Norfolk*	*2/3/2017*
Patricia D. Jehlen	*Second Middlesex*	*2/3/2017*
Thomas M. Stanley	*9th Middlesex*	*2/10/2017*

SENATE DOCKET, NO. 1175 FILED ON: 1/19/2017

SENATE . . . . . No. 943

By Ms. Spilka, a petition (accompanied by bill, Senate, No. 943) of Karen E. Spilka, Jay R. Kaufman, Jason M. Lewis, Thomas M. McGee and other members of the General Court for legislation to update privacy protections for personal electronic information. The Judiciary.

[SIMILAR MATTER FILED IN PREVIOUS SESSION
SEE SENATE, NO. *903* OF 2015-2016.]

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:

SECTION 1. Section 17B of chapter 271 of the General Laws is hereby repealed.

SECTION 2. Chapter 276 of the General Laws, as appearing in the 2014 Official Edition, is hereby amended by striking out section 1B and inserting in place thereof the following section:-

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

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

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

(2) a flight from prosecution;

(3) the destruction of or tampering with evidence;

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

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

"Cell site simulator device", a device that transmits or receives radio waves to simulate an electronic device, cell tower, cell site, or service for the purpose of conducting one or more of the following operations:

(1) identifying, locating or tracking the movements of an electronic device;

(2) intercepting, obtaining, accessing or forwarding the communications, stored data or metadata of an electronic device;

(3) affecting the hardware or software operations or functions of an electronic device;

(4) forcing transmissions from or connections to an electronic device; or

(5) denying an electronic device access to other electronic devices, communications protocols or services.

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

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

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

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

"Location information service", a global positioning service or other mapping, locational or directional information service.

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

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

"Personal electronic information", any of the following or records thereof:

(1) information which, alone or in combination, could reveal the identity of a customer using electronic communication services, remote computing services or location information services;

(2) data stored by or on behalf of a customer;

(3) records of a customer's use of those services identified in (1);

(4) means and source of payment for such services identified in (1), including any credit card or bank account number;

(5) the source of communications sent to a customer or the recipient of communications sent from a customer;

(6) any content of communications stored or transmitted by an electronic communication or remote computing service;

(7) internet protocol addresses;

(8) metadata;

(9) location information; or

(10) the records of (1) through (9).

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

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

"Subpoena", a grand jury or trial subpoena issued in the course of a criminal proceeding.

(b) A government office or public official may obtain or access personal electronic information only (i) with a person's informed consent, (ii) pursuant to a warrant issued by a judicial officer upon an application demonstrating probable cause, (iii) pursuant to a valid subpoena issued pursuant to this section or (iv) acting in accordance with a legally recognized exception to the warrant requirement.

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

(d) Upon complaint on oath that the complainant believes that the use of a cell site simulator device will lead to (i) evidence of or the means or instrumentalities of the commission of a specified criminal offense under the laws of the commonwealth or (ii) the location of a person whom there is probable cause to believe has committed, is committing or is about to

commit a crime, a justice of the superior court may, if satisfied that probable cause has been established for such belief, issue a warrant authorizing that particular personal electronic information be sought from a specified electronic device or if the complainant is unable to specify the particular device, from electronic devices at a specified location, stating the duration for authorized use of the cell site simulator device, and directing the person authorized by the warrant to take all other actions prescribed by this section.

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

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

(e) Search warrants issued under this section shall designate the person, corporation or other entity, if any, in possession of the records or data sought, and shall describe, with particularity, the personal electronic information sought and to be provided. They shall be issued in the form and manner prescribed in sections 2A½ and 2B, if applicable, and shall be directed to the law enforcement officer or government office making application for the warrant.

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

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

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

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

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

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

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

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

(i) A law enforcement officer or agency authorized to use a cell site simulator device in accordance with this section shall: (i) take all steps necessary to limit the collection of any personal electronic information to the target specified in the application and warrant authorization; (ii) take all steps necessary to permanently delete any personal electronic information collected from any person or persons not specified in the warrant immediately following such collection and ensure that such information is not used, retained or transmitted for any purpose; and (iii) delete any information collected from the person or persons specified in the warrant authorization within 30 days if there is no longer probable cause to support the belief that such information is evidence of a crime.

(j) Not later than 7 days after information is obtained by a law enforcement officer or government office pursuant to a warrant under this section, that officer or office shall serve upon

or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the warrant, to the customer or subscriber or user of an electronic device targeted by a cell site simulator device, a copy of the warrant, a copy of the application for the warrant and notice that informs the customer, subscriber, or user of the following:

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

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

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

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

(5) which court made the certification or determination under which a delay under subsection (k) was made, if applicable.

(k) A government office or public official may include in its application for a warrant a request for an order delaying the notification required under subsection (j) for a period not to exceed 90 days and the court may issue the order if it determines there is reason to believe that

notification of the existence of the warrant may have an adverse result. Upon expiration of any period of delay granted under this subsection, the government office or public official shall provide the customer or subscriber a copy of the warrant together with notice required under and by the means described in subsection (j).

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

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

(l) Notwithstanding any general or special law to the contrary, a government office or public official may obtain personal electronic information:

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

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

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

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

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

(m) On the second Friday of January of each calendar year, any judge issuing or denying a subpoena, warrant, or emergency request under this section during the preceding calendar year shall report on each to the office of court management within the trial court:

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

(2) the offense specified in the application;

(3) the nature of the information sought;

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

(5) if the application sought authorization to obtain or access information from a corporation or other entity, the name of that entity;

(6) whether the warrant, subpoena, or emergency request was granted as applied for, was modified or was denied;

(7) the period of disclosures or access authorized;

(8) the number and duration of any extensions; and

(9) any order directing delayed notification of the warrant's existence.

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

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

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

SECTION 3. Chapter 276 is hereby amended by inserting after section 2A the following section:-

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

THE COMMONWEALTH OF MASSACHUSETTS.

(COUNTY), ss. (NAME) COURT.

To the (person or persons or offices authorized to execute the warrant issued under section 1B of chapter 276 of the General Laws).

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

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

(description of particular records or data),

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

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

Justice of the Superior Court

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

THE COMMONWEALTH OF MASSACHUSETTS.

(COUNTY), ss. (NAME) COURT.

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

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

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

(description of particular records or data),

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

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

Justice of the Superior Court

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

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

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