SENATE DOCKET, NO. 1786 FILED ON: 1/16/2015

SENATE . . . . . No. 298

The Commonwealth of Massachusetts

PRESENTED BY:

Patricia D. Jehlen

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 protecting student privacy.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
Patricia D. Jehlen	*Second Middlesex*
Carolyn C. Dykema	*8th Middlesex*
James B. Eldridge	*Middlesex and Worcester*

SENATE DOCKET, NO. 1786 FILED ON: 1/16/2015

SENATE . . . . . No. 298

By Ms. Jehlen, a petition (accompanied by bill, Senate, No. 298) of Patricia D. Jehlen, Carolyn C. Dykema and James B. Eldridge for legislation to protect student privacy. Education.

The Commonwealth of Massachusetts

In the One Hundred and Eighty-Ninth General Court
(2015-2016)

An Act protecting student 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. Chapter 71 of the General Laws are hereby amended by inserting, after section 94, the following new section:-

Section 95. (a) For the purposes of this section, the following words shall have the following meanings:--

"Personally identifiable student data", one or more of the following:

(1) A student's name;

(2) The name of a student's parent, legal guardian, or other family member;

(3) The address of a student or student's parent, legal guardian, or other family member;

(4) Indirect identifiers, including a student's date of birth, place of birth, social security number, telephone number, credit card account number, insurance account number, financial services account number, email address, social media address, and other electronic address; or

(5) Any other information that, alone or in combination, is linked or linkable to a specific student that would allow a third party to identify the student with reasonable certainty.

"Personal device", a technological device owned, leased, or lawfully possessed by a student that was not provided to the student by the school or school district.

"Technological device", any computer, cellular phone, smartphone, digital camera, video camera, audio recording device, or other electronic device that can be used for creating, storing, or transmitting information in the form of electronic data.

"Third party", any person or entity other than a school employee, student, or parent or legal guardian of a student.

(b) Educational institutions shall have the discretion to limit or prohibit the possession or use of certain personal devices by students on school property. A violation of such a limitation or prohibition shall not be the sole basis for a reasonable suspicion to access the device.

(c) No school employee or third party shall access any data or other content input into or stored upon a personal device of a student, notwithstanding any violation of school code of conduct provisions regarding possession or use of such device, unless:

(1) A school employee has a reasonable suspicion that a student has violated or is violating a separate provision of the code of conduct and that the device contains evidence thereof, subject to the following limitations:

(i) Searches of shall be conducted only of personal devices located on school property.

(ii) Prior to searching a student's personal device based on reasonable suspicion, the school employee shall document such reasonable suspicion and notify the student and the

student's parent or legal guardian of the suspected violation and the type of data sought to be accessed in searching for evidence of the violation.

(iii) Searches of a student's personal device based on reasonable suspicion shall be strictly limited to locating evidence of the particular suspected policy violation.

(iv) Where a student is suspected of conduct which is a criminal offense under the general laws, no search shall be undertaken without the authorization of a valid judicial warrant secured in accordance with subsection (c)(2), notwithstanding any suspected violation of the school code of conduct.

(2) Authorized by a valid warrant for the search of the device issued pursuant to the requirements of sections 2 through 3A of chapter 276; or

(3) Accessing a student's personal device is necessary in response to an imminent threat to life or safety. Within 72 hours of accessing a personal device in response to an imminent threat to life or safety, the school employee or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the particular threat and the data accessed.

(d) Each educational institution shall maintain a personal device access log in which the following information shall be recorded for each search of a student's personal device under subsection (c) by school employees or third parties: the name of the school official or third party accessing the device; the date of access; the data or functions accessed; and the basis for the search. Personal device access logs maintained pursuant to this provision shall not contain any personally identifiable student data and shall be public records. Each educational institution shall review its personal device access log annually to ensure compliance with this section,

identify any inappropriate access to personal devices, and formulate and implement an appropriate response.

(e) Evidence or information obtained or collected in violation of this section shall not be admissible as evidence in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing.