SENATE DOCKET, NO. 1797 FILED ON: 1/19/2023

# SENATE . . . . . No. 280

## The Commonwealth of Massachusetts

PRESENTED BY:

***Barry R. Finegold***

*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 relative to student and educator data privacy.

PETITION OF:

| NAME: | DISTRICT/ADDRESS: |
|---|---|
| *Barry R. Finegold* | *Second Essex and Middlesex* |

SENATE DOCKET, NO. 1797 FILED ON: 1/19/2023

# SENATE . . . . . No. 280

By Mr. Finegold, a petition (accompanied by bill, Senate, No. 280) of Barry R. Finegold for legislation relative to student and educator data privacy. Education.

## The Commonwealth of Massachusetts

**In the One Hundred and Ninety-Third General Court**
**(2023-2024)**

An Act relative to student and educator data 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 is hereby amended by inserting after section 34H the following four sections:-

Section 34I. As used in sections 34I through 34L, the following words shall, unless the context clearly requires otherwise, have the following meanings:

"Aggregated data", data collected and reported at the group, cohort, school, school district, region or state level that is aggregated using protocols that are both intended and reasonably likely to preserve the anonymity of each individual.

"Board", the board of elementary and secondary education.

"Commissioner", the commissioner of the department of elementary and secondary education.

"Covered information", information, data or records, inclusive of student records as defined in the board's regulations, that, alone or in combination, can be used to identify a specific student, teacher, principal, administrator or student's family member and that is: (i) created by or provided to an operator by a student, or the student's parent or legal guardian, in the course of the student's, parent's or legal guardian's use of the operator's site, service or application for K-12 school purposes; (ii) created by or provided to an operator by an employee or agent of a school district or K-12 school for K-12 school purposes; (iii) gathered by an operator through the operation of its site, service or application for K-12 school purposes and personally identifies a student; or (iv) gathered by an operator through the operation of its site, service or application in connection with performance evaluations conducted pursuant to section 38 of this chapter and that personally identifies a teacher, principal or administrator.

For a student, covered information includes, but is not limited to, information in the student's educational record or electronic mail, including student-generated work; first and last name; home address and geolocation information; telephone number; electronic mail address or other information that allows physical or online contact; discipline records; test results, grades and student evaluations; special education data; juvenile dependency records; criminal records; medical records and health records; social security number; student identifiers; biometric information; socioeconomic information; food purchases; political and religious affiliations; text messages; student identifiers; search activity and online behavior or usage of applications when linked or linkable to a student; photographs; voice recordings; and persistent unique identifiers.

"De-identified data", records and information from which all personally identifiable information has been removed or obscured such that the remaining information does not

reasonably identify a specific individual, including, but not limited to, any information that alone or in combination is linkable to a specific individual.

"Department", the department of elementary and secondary education.

"Destroy", action taken in the normal course of business that is intended, and what a reasonable person would believe in the context of the information's medium, to make such information permanently irretrievable.

"District" or "school district", the school department of a city or town, regional school district, vocational or agricultural school, independent vocational school or charter school.

"Educational entity", a state educational agency, school district, K-12 school or subdivision thereof, education collaborative as defined in section 4E of chapter 40, approved public or private day and residential school providing special education services to publicly funded eligible students pursuant to chapter 71B or institutional K-12 school program overseen by a state agency including the department of youth services, the department of mental health or the department of public health as well as employees acting under the authority or on behalf of an educational entity.

"K-12 school", a school that offers any of grades kindergarten to 12 and that is operated by a school district; provided, further, that a K-12 school shall include any preschool or prekindergarten program or course of instruction provided by a school district.

"K-12 school purposes", uses that are directed by or that customarily take place at the direction of a school district, K-12 school or teacher or that aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative

activities and collaboration between students, school personnel or parents, or that are otherwise for the use and benefit of the K-12 school; provided, further, that K-12 school purposes shall include comparable purposes in the administration of any preschool or prekindergarten program or course of instruction provided by a school district.

"Operator", a person or entity operating in accordance with an agreement with an educational entity to provide an Internet website, online service, online application or mobile application for K-12 school purposes or at the direction of an educational entity or an employee of an educational entity; provided, however, that this definition shall not apply to the department, school district, K-12 school or other educational entity.

"Persistent unique identifier", an identifier that can be used to recognize a consumer, a family or a device that is linked to a consumer or family over time and across different services, including, but not limited to: (i) a device identifier; (ii) an Internet Protocol address; (iii) cookies, beacons, pixel tags, mobile ad identifiers or similar technology; (iv) customer number, unique pseudonym or user alias; or (v) telephone number or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device; provided, however, that for the purposes of this definition "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

"Targeted advertising", presenting or serving advertisements to a student where the substance, time or manner of the advertisement is determined based in whole or in part on information obtained or inferred over time from that student's online behavior, usage of applications or covered information. It does not include advertising to a student at an online location based upon that student's current visit to that location or in response to that student's

request for information or feedback without the retention of that student's online activities or requests over time for the purpose of targeting subsequent advertisements.

Section 34J. (a) An operator shall not, with respect to its site, service or application:

(1) engage in targeted advertising on the operator’s site, service or application, or targeted advertising on any other site, service or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, that the operator has acquired because of the use of that operator's site, service or application for K-12 school purposes;

(2) use covered information, including persistent unique identifiers, created or gathered by the operator's site, service or application, to amass a profile about a student or a teacher, principal or administrator except in furtherance of K-12 school purposes;

(3) sell or rent a student’s information, including covered information; provided, however, that this subsection shall not apply to the purchase, merger or other type of acquisition of an operator by another entity, if the operator or successor entity complies with sections 34I through 34L of this chapter, or to national assessment providers if the national assessment provider secures the express written consent of the parent or student if 18 years old, given in response to clear and conspicuous notice solely to provide access to employment, educational scholarships or financial aid or postsecondary educational opportunities; or

(4) disclose covered information; provided, however, that an operator may disclose covered information of a student so long as clauses (1) through (3), inclusive, of this subsection are not violated, under the following circumstances:

(i) if provisions of federal or state law require the operator to disclose the information, and the operator complies with the requirements of federal and state law in protecting and disclosing that information;

(ii) for research purposes with the approval of the relevant educational entity and in compliance with and subject to the restrictions of state and federal law; provided, however, that the information shall be de-identified prior to being disclosed and that the operator shall share research results with the educational entity in advance of any public dissemination; or

(iii) to an educational entity, including a K-12 school and school district, for K-12 school purposes, as permitted by state or federal law.

(b) An operator shall:

(1) implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information designed to protect that covered information from unauthorized access, destruction, use, modification or disclosure and in compliance with regulations promulgated by the board pursuant to section 34L of this chapter; and

(2) immediately return or destroy covered information if requested by the educational entity or when covered information is no longer required for K-12 school purposes or other lawful purposes, such as complying with a judicial order or law enforcement request.

(c) Subject to the provisions of this section, an operator may use de-identified data to maintain, develop, support, improve or diagnose the operator’s site, service or application. Subject to the provisions of this section, an operator may use aggregated or de-identified student information to demonstrate the effectiveness of the operator’s products or services, including

marketing or within the operator's site, service or application or other sites, services or applications owned by the operator to improve educational purposes.

(d) Nothing in this section shall be construed to: (1) limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction; (2) limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes; (3) apply to general audience Internet websites, general audience online services, general audience online applications or general audience mobile applications, even if login credentials created for an operator's site, service or application may be used to access those general audience sites, services or applications; (4) limit service providers from providing Internet connectivity to schools or students and their families; (5) prohibit an operator of an Internet website, online service, online application or mobile application from marketing educational products directly to parents if the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this section; (6) impose a duty upon a provider of an electronic store, gateway, marketplace or other means of purchasing or downloading software or applications to review or enforce compliance with this section on those applications or software; or (7) prohibit students from downloading, exporting, transferring, saving or maintaining their own data or documents.

(e) An aggrieved student or educational entity may institute a civil action against an operator for damages or to restrain a violation of this section and may recover: (1) up to $10,000 for each disclosure that violates this section; (2) up to $10,000 for each adverse action that violates this section, or actual damages, whichever amount is higher; (3) punitive damages if a

court determines that a violation was willful; and (4) reasonable attorneys' fees and other litigation costs reasonably incurred.

(f) The commissioner may bar an operator that improperly discloses covered information from receiving access to student and educator evaluation records of any educational entity in the commonwealth for a period of no less than five years.

Section 34K. (a) Any contract or agreement that is entered between an educational entity and an operator, as defined in section 34I, pursuant to which the operator sells, leases, provides, operates or maintains a service that grants access to covered information or creates any covered information, including, but not limited to (i) any cloud-based services for the digital storage, management and retrieval of pupil records or (ii) any digital software that authorizes an operator to access and acquire student records, shall contain:

(1) a description of the covered information collected, stored and managed and a statement that covered information and student records continue to be the property and under the control of the educational entity;

(2) a prohibition against the operator using covered information for commercial or advertising purposes or for any purpose other than K-12 school purposes;

(3) a description of the procedures by which a parent, legal guardian or eligible student may review the student's records and work with the educational entity to correct erroneous information, in accordance with state and federal law;

(4) a requirement that only persons, whether they are employees of the operator or other persons, such as employees of subcontractors, with a legitimate need to access covered

information to support professional roles consistent with the terms of the contract or agreement and federal and state law shall have access to it, with either the identification of said persons or an agreement to identify said persons upon request;

(5) a description of the reasonable administrative, technical and physical safeguards including with respect to encryption technology to protect covered information while in motion or in the operator's custody that the operator will employ to protect the security, confidentiality and integrity of covered information in its custody; provided, however, compliance with this requirement shall not, in itself, absolve the operator of liability in the event of an unauthorized disclosure of covered information;

(6) a description of the procedures for notifying any and all affected parties in the event of an unauthorized disclosure of covered information or any breach of security resulting in an unauthorized release of covered information, provided that the procedures shall comply with chapter 444 of the acts of 2018 and implementing regulations;

(7) a certification that covered information shall be returned or destroyed by the operator upon completion of the terms of the contract; and

(8) a description of how the educational entity and the operator will jointly ensure compliance with applicable federal and state law, including, but not limited to, 20 U.S.C. section 1232g, 15 U.S.C. section 6501 et. seq. and sections 34A through 34L, inclusive, of this chapter.

(b) Any contract that fails to comply with the requirements of this section shall be voidable and all covered information and student records in possession of an operator or any third party shall be returned to the educational entity or, if the return of such information is not technologically feasible, destroyed.

Section 34L. (a) The board shall promulgate regulations that establish data security and privacy responsibilities of the department and educational entities as well as minimum required security standards for operators, including for use in department and educational entity contracts and agreements with operators, and shall approve the department's data privacy and security policy and security plan for the state data system. The regulations further shall establish the process through which the commissioner, pursuant to subsection (g) of section 34J, may bar an operator from receiving student and educator evaluation data of any educational entity in this commonwealth for a period of no less than five years. The regulations further shall provide that curricula in student data privacy, security and confidentiality shall be a requirement for approved educator preparation programs. In carrying out these responsibilities, the board shall consult with the executive office of technology services and security and seek the input of security and cybersecurity experts, including those from fields in addition to education that have experience with personal data protection.

(b) The commissioner shall appoint a chief privacy officer with experience in data privacy and security. The chief privacy officer shall oversee the development and implementation, subject to the board's approval, of a department data privacy and security policy and a detailed security plan for the state data system in consultation with the executive office of technology services and security. The chief privacy officer further shall develop a model school district data privacy and security policy as well as a model operator contract or contracts in consultation with the executive office of technology services and security; otherwise support and supervise implementation of sections 34I through 34L, inclusive, of this chapter and the regulations issued by the board pursuant to subsection (a); develop and provide a program of training, technical assistance and resource materials to K-12 schools, school districts and other

educational entities including through the issuance of guidance and recommendations to assist with compliance with federal and state law pertaining to personally identifiable information including, but not limited to, 20 U.S.C. 1232g, sections 34A through 34L, inclusive, of chapter 71 of the General Laws, chapter 66A of the General Laws and chapter 444 of the acts of 2018; develop and oversee a program of oversight, support and accountability for the department and educational entities responsible for implementing policies pursuant to sections 34I through 34L of this chapter; and assist the commissioner with enforcement responsibilities regarding operators that violate any provision of sections 34I through 34K, inclusive, of this chapter.

(c) The department shall make publicly available a list of categories of covered information collected by the department including, but not limited to, covered information required to be collected or reported by state or federal law. The list shall contain the source of the information, the reason for the collection of the information and the use of the information collected.

(d) In accordance with the regulations of the board promulgated pursuant to subsection (a), each district shall develop a detailed privacy and security policy for the protection of covered information that includes security breach planning, notice and procedures; provided, however, that said policy shall include a requirement that the district report all significant data breaches of student data either by the district or an operator to the commissioner within ten business days of the initial discovery of the significant data breach; and provided, further, that a district may adopt any model policy developed by the chief privacy officer of the department and approved by the board to comply with this requirement. Each district shall designate an individual to act as a student data manager to oversee said policy.

(e) Each district shall make publicly available on its website a list of categories of student personally identifiable information collected at the school district, school or classroom level. The list shall contain the source of the information, the reason for collection of the information and the use of the information. Each district further shall make publicly available on its website a list of the operators with which the district has a contract or agreement that involves the creation, provision or gathering of covered information and a list of operators with which the district had a contract or agreement that involved the creation, provision or gathering of covered information in the last ten years.

(f) Each district annually shall provide annual training regarding the confidentiality of student data to any employee with access to covered information; provided that, completion of said training shall be a condition of a provisional or standard educator certification as defined in section 38G.