SPONSOR: Sen. Sokola & Rep. Jaques & Rep. Ramone
Sens. Henry, Marshall, Peterson; Reps. Briggs King, Keeley, Lynn, Matthews, Miro, Osienski, K. Williams

DELAWARE STATE SENATE
148th GENERAL ASSEMBLY

SENATE SUBSTITUTE NO. 1

FOR

SENATE BILL NO. 79

AN ACT TO AMEND TITLE 14 OF THE DELAWARE CODE RELATING TO EDUCATIONAL DATA GOVERNANCE.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE:

Section 1. Amend Part V, Title 14 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underline as follows:

Chapter 81A. Student Data Privacy Protection Act.

§ 8101A. Short title.

This chapter shall be known and may be cited as the "Student Data Privacy Protection Act."

§ 8102A. Definitions.

For purposes of this chapter:

(1) "Aggregate student data" means data that is not personally identifiable and that is collected or reported at the group, cohort, or institutional level.

(2) "De-identified data" means a student data set that cannot reasonably be used to identify, contact, single out, or infer information about a student or a device used by a student.

(3) "Department" means the Delaware Department of Education.

(4) "Education record" means an education record as defined in the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and its implementing regulations, 34 C.F.R. Part 99, as amended.

(5) "Geolocation data" means information that is, in whole or part, generated by, derived from, or obtained by the operation of an electronic device that can be used to identify the past, present, or future location of an electronic device, an individual, or both.

(6) "Internet" means, collectively, the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ

the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

(7) "K-12 school purposes" means purposes that customarily take place at the direction of a school, teacher, or school district or aid in the administration of school activities, including instruction in the classroom or at home, administrative activities, preparing for postsecondary education or employment opportunities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school.

(8) "Law enforcement entity" means any government agency or any subunit thereof which performs the administration of criminal justice pursuant to statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice, including the Delaware State Police, all law enforcement agencies and police departments of any political subdivision of this State, the Department of Correction, and the Department of Justice.

(9) "Online contact information" means an e-mail address or any other substantially similar identifier that permits direct contact with an individual online, including an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, a video chat user identifier, or a screen name or user name that permits such contact.

(10) "Operator" means any person other than the Department, school districts, or schools, to the extent that the person does any of the following:

a. Operates an Internet website, online or cloud computing service, online application, or mobile application with actual knowledge that the Internet website, online or cloud computing service, online application, or mobile application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes.

b. Collects, maintains, or uses student data in a digital or electronic format for K-12 school purposes.

(11) "Parent" means a student's parent, legal guardian, or relative caregiver pursuant to § 202(f) of this title.

(12) "School" means any public school in the State providing educational instruction in one or more grades from kindergarten through grade 12.

(13) "School district" means a clearly defined geographical subdivision of the State organized for the purpose of administering public education in that area.

(14) "State-assigned student identifier" means the unique student identifier assigned by the State to each student that shall not be and shall not include the social security number of a student in whole or in part.

(15) "Student" means any individual attending a school in this State.

(16) "Student data" means personally identifiable information or materials, in any media or format, that meets any of the following:

a. Is student performance information.

b. Is created or provided by a student or parent to an employee or agent of the Department, school district, or school.

c. Is created or provided by a student or parent to an operator in the course of the student's or parent's use of the operator's site, service, or application for K-12 school purposes.

d. Is created or provided by an employee or agent of a school district or school, to an operator.

e. Is gathered by an operator through the operation of a site, service, or application described in paragraph (10)a. of this section and can be used to distinguish or trace the identity of the student, or is linked to information that can be used to distinguish or trace the identity of the student, including information in the student's education record or email; the student's name, in whole or in part; residential or other address that allows physical contact; telephone number; online contact information; discipline records; test results; special education data; juvenile dependency records; criminal records; medical records; health records; social security number; passport number; student identification number or other student identifier; driver's license number; state identification card number; alien registration number; geolocation data; biometric information; disability status; socioeconomic information; food purchases; political affiliations; religious information; text messages; instant messages; documents; search activity; photos; voice recordings; or video recordings.

(17) "Student performance information" means the following data relating to student performance from early childhood learning programs through postsecondary education: college and career readiness; course and grade; degree, diploma, or credential attainment, including high school equivalency diploma; demographic; educator; enrollment; financial aid; remediation; retention; state and national assessments; transcripts; vocational and technical education information; any other data relating to education deemed necessary by the Department.

(18) "Targeted advertising" means presenting advertisements to a student, or a student's parent, where the advertisement is selected based on information obtained or inferred from that student's online behavior, usage of applications, or student data. "Targeted advertising" does not include advertising to a student at an online location based upon that student's current visit to that location without collection and retention of a student's online activities over time.

§ 8103A. Enforcement.

The Consumer Protection Unit of the Department of Justice has enforcement authority over this chapter and may investigate and prosecute violations of this chapter in accordance with the provisions of subchapter II of Chapter 25 of Title 29 of the Delaware Code.

§ 8104A. Operator duties.

An operator shall:

(1) Implement and maintain reasonable security procedures and practices appropriate to the nature of the student data to protect that information from unauthorized access, destruction, use, modification, or disclosure, which shall, at a minimum, comply with the Department of Technology and Information's Cloud and Offsite Hosting Policy and include the terms and conditions set forth in the Department of Technology and Information's Cloud and Offsite Hosting Template for Non-Public Data.

(2) Delete a student's data within a reasonable timeframe not to exceed 45 calendar days if a school district or school requests deletion of data under the control of the school district or school.

§ 8105A. Operator prohibited activities.

An operator shall not knowingly engage in any of the following activities with respect to such operator's Internet website, online or cloud computing service, online application, or mobile application:

(1) Engage in targeted advertising on the operator's, or any other, Internet website, online or cloud computing service, online application, or mobile application when the targeting of the advertising is based upon any information, including student data and state-assigned student identifiers or other persistent unique identifiers, that the operator has acquired because of the use of an Internet website, online or cloud computing service, online application, or mobile application as described in § 8102A(10)a. of this title.

(2) Use information, including state-assigned student identifiers or other persistent unique identifiers, created or gathered by an Internet website, online or cloud computing service, online application, or mobile application as described in § 8102A(10)a. of this title, to amass a profile about a student except in furtherance of K-12 school purposes.

(3) Sell student data. This prohibition does not apply to the purchase, merger, or other type of acquisition of an operator by another entity, provided that the operator or successor entity continues to be subject to the provisions of this chapter with respect to previously-acquired student data that is subject to this chapter.

(4) Disclose student data, unless the disclosure is made for any of the following reasons:

a. In furtherance of the K-12 school purposes of the Internet website, online or cloud computing service, online application, or mobile application. The recipient of the student data disclosed for this reason shall not further disclose the student data unless done to allow or improve the operability and functionality within that student's classroom or school, and is legally required to comply with the requirements of § 8104A of this title or paragraphs (1) through (3) of this section.

b. To ensure legal or regulatory compliance.

c. To respond to or participate in judicial process.

d. To protect the security or integrity of the operator's Internet website, online or cloud computing service, online application, or mobile application.

e. To protect the safety of users or others or security of the Internet website, online or cloud computing service, online application, or mobile application.

f. To a service provider, provided that the operator, by contract, does all of the following:

1. Prohibits the service provider from using any student data for any purpose other than providing the contracted service to, or on behalf of, the operator.

2. Prohibits the service provider from disclosing to subsequent third parties any student data provided by the operator.

3. Requires the service provider to comply with the requirements of paragraphs (1) through (3) of this section and to implement and maintain the security procedures and practices as provided in § 8104A(1) of this title.

(5) Notwithstanding paragraph (4) of this section, an operator may disclose student data under the following circumstances, so long as paragraphs (1) through (3) of this section are not violated:

a. When another provision of state or federal law requires the operator to disclose the student data, and the operator complies with the requirements of applicable state and federal law in protecting and disclosing that information.

b. For legitimate research purposes:

1. As required by state or federal law and subject to the restrictions under applicable state or federal law.

2. As allowed by state or federal law and under the direction of a school district, school, or the Department, if no student data is used for any purpose in furtherance of advertising or to amass a profile on the student for purposes other than K-12 school purposes.

c. To a state agency, school district, or school, for K-12 school purposes, as permitted by state or federal law.

(6) Nothing in this subsection prohibits an operator from using student data for any of the following:

a. Maintaining, delivering, supporting, evaluating, or diagnosing the operator's Internet website, online or cloud computing service, online application, or mobile application.

b. Adaptive learning or customized student learning purposes.

(7) Nothing in this subsection prohibits an operator from using or sharing aggregate student data or de-identified student data for any of the following:

a. The development and improvement of the operator's Internet website, online or cloud computing service, online application, or mobile application, or other educational Internet websites, online or cloud computing services, online applications, or mobile applications.

b. Within other Internet websites, online or cloud computing services, online applications, or mobile applications owned by the operator, and intended for school district, school, or student use, to evaluate and improve educational products or services intended for school district, school, or student use.

c. To demonstrate the effectiveness of the operator's products or services, including their marketing.

§ 8106A. Exclusions.

This chapter shall not be construed so as to do any of the following:

(1) Apply to general audience Internet websites, online or cloud computing services, online applications, or mobile applications, even if login credentials created for an operator's Internet website, online or cloud computing service, online application, or mobile application may be used to access those general audience Internet websites, online or cloud computing services, online applications, or mobile applications.

(2) Limit the authority of a law enforcement agency to obtain any content or student data from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

(3) Limit Internet service providers from providing Internet connectivity to schools or students and their families.

(4) Prohibit an operator from marketing educational products directly to parents, so long as the marketing does not result from the use of student data obtained by the operator through the provision of services covered under this chapter.

(5) 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 chapter on those applications or software.

(6) Impose a duty upon a provider of an interactive computer service, as defined in § 230 of Title 47 of the United States Code, to review or enforce compliance with this chapter by third-party content providers.

(7) Impede the ability of a student or parent or guardian to download, transfer, export, or otherwise save or maintain their own student data or documents.

(8) Prevent the Department, school district, or school from recommending, solely for K-12 school purposes, any educational materials, online content, services, or other products to any student or to the student's family if the Department, school district, or school determines that such products will benefit the student and no person receives compensation for developing, enabling, or communicating such recommendations.

Section 2. The provisions of Section 1 of this Act do not apply to projects relating to the privacy and security of student data approved prior to the effective date of this Act under the Department of Education's data governance regulation, § 294, Title 14 of the Delaware Administrative Code, in existence on the effective date of this Act.

Section 3. There is established a Student Data Privacy Task Force to study and make findings and recommendations regarding the development and implementation of a comprehensive framework to govern the privacy, protection, accessibility, and use of student data within and as part of the State's public education system. The Task Force is composed of the Attorney General, the Secretary of Education, the President of the State Board of Education, the Secretary of the Department of Technology and Information, the Chief of the State School Officers Association, the President of the Delaware School Boards Association, the President of the Delaware Charter Schools Network, the President of the Delaware State Education Association, and the President of the Delaware Congress of Parents & Teachers, Inc., or their respective designees, and two representatives from companies, trade associations, or groups which operate in the area of student data privacy or online educational technology services, appointed by the Chairs of the Education Committees of the Senate and House of Representatives. The chair of the Task Force shall be the Attorney General, or the Attorney General's designee, who shall be responsible for the administration of the Task Force. The Department of Justice shall be responsible for providing reasonable and necessary support staff and materials for the Task Force. The Task Force shall report its findings and recommendations in writing to the Chairs of the Education Committees of the Senate and

House of Representatives, and to the Directors of the Division of Research and the Delaware Public Archives, by December 18, 2015.

Section 4. If any provision of this Act or the application thereof to any person or circumstances is held invalid, the invalidity does not affect any other provision or application of the Act which can be given effect without the invalid provision or application; and, to that end, the provisions of this Act are declared to be severable.

Section 5. Section 1 of this Act becomes effective on August 1 the first full year following the Act's enactment into law. Sections 2 through 4 of this Act become effective upon the Act's enactment into law.

SYNOPSIS

The Student Data Privacy Protection Act will enable students and educators in Delaware public schools to use technology to enhance student educational opportunities without compromising the privacy and security of student data. According to a recent survey of parental attitudes toward educational technology published American Public Media, an overwhelming majority of parents are concerned about the security and privacy of their children's data, how that data is collected and used, and access advertisers will have to children using educational technology.

Modeled after California's groundbreaking Student Online Personal Information Privacy Act, the Student Data Privacy Protection Act prohibits education technology service providers, primarily operators of Internet websites, online or cloud computing services, mobile service, and mobile applications used for K-12 school purposes, from selling student data, using student data to engage in targeted advertising to students or their families, amassing a profile on students to be used for non-educational purposes, or disclosing student data except as permitted by the Act. The Act also requires education technology service providers to have reasonable procedures and practices for ensuring the security of student data they collect or maintain, protecting that student data from unauthorized access, destruction, use, modification, or disclosure, and deleting the student data if appropriately requested to do so by a school or school district.

The Act also establishes a Student Data Privacy Task Force to study and make findings and recommendations regarding the development and implementation of a comprehensive framework to govern the privacy, protection, accessibility, and use of student data at all levels of the State's public education system.

The Act gives the Consumer Protection Unit of the Department of Justice the authority to investigate and prosecute violations of the Act.

The Act exempts any projects relating to student data privacy and security approved under the Department of Education's existing education record privacy regulation prior to the effective date of the Act.

The Act provides that its provisions are severable.

The Act provides that Section 1 will become effective on August 1 the first full year following the Act's enactment into law, while the remaining sections of the Act will become effective immediately upon the Act's enactment into law.

The Act is substituted for Senate Bill No. 79 and differs from Senate Bill No. 79 by (1) creating a new chapter in Title 14 of the Delaware Code creating the "Student Data Privacy Protection Act"; (2) deleting provisions addressing data security and privacy responsibilities of the Department of Education in favor of establishing the Student Data Privacy Task Force to study and report on those issues as part of a comprehensive evaluation of student data privacy and security within the State's public education system; (3) clarifying that an operator's security and privacy procedures must comply with certain terms and conditions required by the Department of Technology and Information for all state online and cloud computing service contracts involving non-public data; (4) clarifying the circumstances under which an operator can use student data for adaptive learning or customized student learning; (5) giving the Department of Justice's Consumer Protection Unit the authority to investigate and prosecute violations of the Act by operators; (6) making the Act's provisions severable; (7) setting different effective dates for Section 1 versus the remaining sections of the Act; (8) revising, adding, and deleting certain definitions; and (9) correcting minor typographical errors.

Author: Senator Sokola