SB3735

LRB10419296LNS32742b

104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

SB3735

Introduced 2/5/2026, by Sen. Robert F. Martwick

SYNOPSIS AS INTRODUCED:

New Act
105 ILCS 5/10-20.40
105 ILCS 5/34-18.34
105 ILCS 85/5
105 ILCS 85/10
105 ILCS 85/15
105 ILCS 85/25

Creates the Student Educational Technologies Rights Act. Provides that it is the policy of the State that a student and the student's parent have the right to: opt out of school-issued personal electronic devices, electronic textbooks, electronic required reading, or electronic or online assignments; request a human teacher review any automated scored grade or scored grade generated by artificial intelligence; and opt out of predictive analytics systems without academic penalty. Amends the School Code. Removes language allowing school districts that collect biometric information from students to adopt specified policies. Prohibits a school district from purchasing or otherwise acquiring biometric systems to use on students. Establishes prohibitions for a school district with respect to biometric systems and biometric information of its students. Sets forth requirements on the destruction of biometric information in the possession of a school district. Makes other changes. Amends the Student Online Personal Protection Act. Prohibits an operator from selling or renting any other person's information collected by the operator for K through 12 school purposes or permitting artificial intelligence to train on covered information unless for K through 12 school purposes or in furtherance of improving operability and functionality of the operator's service. Provides, with exceptions, that an operator's artificial intelligence model shall not train on a student's covered information and retain the training data indefinitely. Makes other and conforming changes.

LRB104 19296 LNS 32742 b

A BILL FOR

AN ACT concerning education.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Student Educational Technologies Rights Act.

Section 5. Legislative findings; intent.

(a) The General Assembly finds all of the following:

(1) Within schools, online services and other technologies to help students learn are now deeply embedded throughout every grade level.

(2) At the same time, there are growing concerns about how student technology use is contributing to youth mental health crises, privacy and security risks, cyberbullying, and reduced attention and ability to focus.

(3) An overwhelming number of parents have expressed that it is growing increasingly difficult to protect their children from the harms online and exasperated by technology use. Because technologies are so prevalent throughout almost every aspect of a child's life, including school, parents face challenges when trying to opt their children out of technology use.

(4) With the introduction of artificial intelligence, students are growing increasingly concerned about the

automation of tasks traditionally performed by a teacher, including grading. When artificial intelligence can hallucinate inaccurate results, students want the ability to ensure they can trust that grading through artificial intelligence or by automation meets the same standards of the teaching profession within this State.

(b) This Act is intended to provide parents with the ability to exercise their parental rights with relation to their child's technology use and provide students and parents with rights associated with educational technologies.

Section 10. Definitions. As used in this Act:

"Artificial intelligence" has the meaning given to that term in Section 2-101 of the Illinois Human Rights Act.

"Parent" has the meaning given to that term under the Section 2 of the Illinois School Student Records Act.

"School" means (i) any preschool, public kindergarten, elementary or secondary educational institution, vocational school, special educational facility, or any other elementary or secondary educational agency or institution or (ii) any person, agency, or institution that maintains school student records from more than one school.

"Student" has the meaning given to that term under Section 2 of the Illinois School Student Records Act.

Section 15. Student educational technology rights.

(a) It is the policy of this State that a student and the student's parent have the right to:

(1) opt out of school-issued personal electronic devices, electronic textbooks, electronic required reading, or electronic or online assignments;

(2) request a human teacher review any automated scored grade or scored grade generated by artificial intelligence; and

(3) opt out of predictive analytics systems without academic penalty.

(b) If a student or a student's parent exercises the right outlined in subsection (a), the school shall provide the student with a comparable analog version of what the educational technology provides.

As used in this subsection, "comparable analog version" includes, but is not limited to, providing the assignment on physical paper, a physical copy of the required reading, or the option of a physical paper textbook.

Section 20. The School Code is amended by changing Sections 10-20.40 and 34-18.34 as follows:

(105 ILCS 5/10-20.40)

Sec. 10-20.40. Student biometric information.

(a) For the purposes of this Section: ~~,~~

"Biometric ~~biometric~~ information" means any information

that is collected through an identification process for individuals based on their unique behavioral or physiological characteristics, including fingerprint, hand geometry, voice, or facial recognition or iris or retinal scans.

"Biometric system" means any combination of hardware, software, firmware, or tools used to obtain, collect, process, store, transmit, display, or otherwise handle biometric information, including, but not limited to, facial or voice recognition software and software to conduct fingerprint, hand geometry, or iris or retinal scans.

"Facial recognition" means any tool using an automated or semiautomated process that assists in uniquely identifying or verifying a person by comparing or analyzing patterns based on the person's face.

(b) A school district is prohibited from purchasing or otherwise acquiring biometric systems, including facial recognition software, to use on students. ~~School districts that collect biometric information from students shall adopt policies that require, at a minimum, all of the following:~~

~~(1) Written permission from the individual who has legal custody of the student, as defined in Section 10-20.12b of this Code, or from the student if he or she has reached the age of 18.~~

~~(2) The discontinuation of use of a student's biometric information under either of the following conditions:~~

~~(A) upon the student's graduation or withdrawal from the school district; or~~

~~(B) upon receipt in writing of a request for discontinuation by the individual having legal custody of the student or by the student if he or she has reached the age of 18.~~

~~(3) The destruction of all of a student's biometric information within 30 days after the use of the biometric information is discontinued in accordance with item (2) of this subsection (b).~~

~~(4) The use of biometric information solely for identification or fraud prevention.~~

~~(5) A prohibition on the sale, lease, or other disclosure of biometric information to another person or entity, unless:~~

~~(A) the individual who has legal custody of the student or the student, if he or she has reached the age of 18, consents to the disclosure; or~~

~~(B) the disclosure is required by court order.~~

~~(6) The storage, transmittal, and protection of all biometric information from disclosure.~~

(b-5) A school district may not do any of the following with respect to students:

(1) Obtain, retain, possess, access, request, or use biometric systems or biometric information derived from biometric systems.

(2) Enter into an agreement with a third party for the purpose of obtaining, retaining, possessing, accessing, or using, by or on behalf of the school district, biometric systems, including facial recognition software or biometric information derived from biometric systems.

(b-10) Within 30 days after the effective date of this amendatory Act of the 104th General Assembly, if a school district is in possession of student biometric information, then the school district shall destroy the biometric information and provide certified documentation of destruction to the State Board of Education.

(b-15) Within 30 days after the effective date of this amendatory Act of the 104th General Assembly, any school district that has contracted with a third party to obtain, collect, or store student biometric information shall require the third party to destroy the biometric information in its possession and confirm in writing the completion of this destruction to the school district.

(b-20) During the 30-day period in which a school district may still have student biometric information in its possession under subsection (b-10), the school district is prohibited from selling, leasing, or otherwise disclosing the biometric information to another person or entity unless:

(1) the individual who has legal custody of the student or the student, if he or she has reached the age of 18, consents to the disclosure; or

(2) the disclosure is required by court order.

(c) (Blank). ~~Failure to provide written consent under item (1) of subsection (b) of this Section by the individual who has legal custody of the student or by the student, if he or she has reached the age of 18, must not be the basis for refusal of any services otherwise available to the student.~~

(d) Student biometric information may be destroyed without notification to or the approval of a local records commission under the Local Records Act if destroyed within 30 days after the effective date of this amendatory Act of the 104th General Assembly ~~use of the biometric information is discontinued in accordance with item (2) of subsection (b) of this Section~~.

(Source: P.A. 95-232, eff. 8-16-07; 95-793, eff. 1-1-09; 95-876, eff. 8-21-08; 96-328, eff. 8-11-09.)

(105 ILCS 5/34-18.34)

Sec. 34-18.34. Student biometric information.

(a) For the purposes of this Section:~~,~~

"Biometric ~~biometric~~ information" means any information that is collected through an identification process for individuals based on their unique behavioral or physiological characteristics, including fingerprint, hand geometry, voice, or facial recognition or iris or retinal scans.

"Biometric system" means any combination of hardware, software, firmware, or tools used to obtain, collect, process, store, transmit, display, or otherwise handle biometric

information, including, but not limited to, facial or voice recognition software and software to conduct fingerprint, hand geometry, or iris or retinal scans.

"Facial recognition" means any tool using an automated or semiautomated process that assists in uniquely identifying or verifying a person by comparing or analyzing patterns based on the person's face.

(b) The school district is prohibited from purchasing or otherwise acquiring biometric systems, including facial recognition software, to use on students. ~~If the school district collects biometric information from students, the district shall adopt a policy that requires, at a minimum, all of the following:~~

~~(1) Written permission from the individual who has legal custody of the student, as defined in Section 10-20.12b of this Code, or from the student if he or she has reached the age of 18.~~

~~(2) The discontinuation of use of a student's biometric information under either of the following conditions:~~

~~(A) upon the student's graduation or withdrawal from the school district; or~~

~~(B) upon receipt in writing of a request for discontinuation by the individual having legal custody of the student or by the student if he or she has reached the age of 18.~~

~~(3) The destruction of all of a student's biometric information within 30 days after the use of the biometric information is discontinued in accordance with item (2) of this subsection (b).~~

~~(4) The use of biometric information solely for identification or fraud prevention.~~

~~(5) A prohibition on the sale, lease, or other disclosure of biometric information to another person or entity, unless:~~

~~(A) the individual who has legal custody of the student or the student, if he or she has reached the age of 18, consents to the disclosure; or~~

~~(B) the disclosure is required by court order.~~

~~(6) The storage, transmittal, and protection of all biometric information from disclosure.~~

(b-5) The school district may not do any of the following with respect to students:

(1) Obtain, retain, possess, access, request, or use biometric systems or biometric information derived from biometric systems.

(2) Enter into an agreement with a third party for the purpose of obtaining, retaining, possessing, accessing, or using, by or on behalf of the school district, biometric systems, including facial recognition software or biometric information derived from biometric systems.

(b-10) Within 30 days after the effective date of this

amendatory Act of the 104th General Assembly, if the school district is in possession of student biometric information, then the school district shall destroy the biometric information and provide certified documentation of destruction to the State Board of Education.

(b-15) Within 30 days after the effective date of this amendatory Act of the 104th General Assembly, if the school district has contracted with a third party to obtain, collect, or store student biometric information, then the school district shall require the third party to destroy the biometric information in its possession and confirm in writing the completion of this destruction to the school district.

(b-20) During the 30-day period in which the school district may still have student biometric information in its possession under subsection (b-10), the school district is prohibited from selling, leasing, or otherwise disclosing the biometric information to another person or entity unless:

(1) the individual who has legal custody of the student or the student, if he or she has reached the age of 18, consents to the disclosure; or

(2) the disclosure is required by court order.

(c) (Blank). ~~Failure to provide written consent under item (1) of subsection (b) of this Section by the individual who has legal custody of the student or by the student, if he or she has reached the age of 18, must not be the basis for refusal of any services otherwise available to the student.~~

(d) Student biometric information may be destroyed without notification to or the approval of a local records commission under the Local Records Act if destroyed within 30 days after the effective date of this amendatory Act of the 104th General Assembly ~~use of the biometric information is discontinued in accordance with item (2) of subsection (b) of this Section~~.

(Source: P.A. 95-232, eff. 8-16-07; 95-793, eff. 1-1-09; 95-876, eff. 8-21-08.)

Section 25. The Student Online Personal Protection Act is amended by changing Sections 5, 10, 15, and 25 as follows:

(105 ILCS 85/5)

Sec. 5. Definitions. In this Act:

"Artificial intelligence" has the meaning given to that term in Section 2-101 of the Illinois Human Rights Act.

"Breach" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of covered information maintained by an operator or school. "Breach" does not include the good faith acquisition of personal information by an employee or agent of an operator or school for a legitimate purpose of the operator or school if the covered information is not used for a purpose prohibited by this Act or subject to further unauthorized disclosure.

"Covered information" means personally identifiable

information or material or information or data that is gathered from personally identifiable information or material through artificial intelligence or information that is linked to personally identifiable information or material in any media or format that is not publicly available and is any of the following:

(1) Created by or provided to an operator by a student or the student's parent in the course of the student's or parent's use of the operator's site, service, or application for K through 12 school purposes.

(2) Created by or provided to an operator by an employee or agent of a school or school district for K through 12 school purposes.

(3) Gathered by an operator through the operation of its site, service, or application for K through 12 school purposes and personally identifies a student, including, but not limited to, information in the student's educational record or electronic mail, first and last name, home address, telephone number, electronic mail address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, a social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text

messages, documents, student identifiers, search activity, photos, voice recordings, ~~or~~ geolocation information, digital replicas, or data collected through the use of artificial intelligence.

"Digital replica" has the meaning given to that term in Section 5 of the Right of Publicity Act.

"Interactive computer service" has the meaning ascribed to that term in Section 230 of the federal Communications Decency Act of 1996 (47 U.S.C. 230).

"K through 12 school purposes" means purposes that are directed by or that customarily take place at the direction of a school, teacher, or school district; 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 are otherwise for the use and benefit of the school.

"Longitudinal data system" has the meaning given to that term under the P-20 Longitudinal Education Data System Act.

"Operator" means, to the extent that an entity is operating in this capacity, the operator of an Internet website, online service, online application, ~~or~~ mobile application, or artificial intelligence model with actual knowledge that the site, service, ~~or~~ application, or model is used primarily for K through 12 school purposes and was designed and marketed for K through 12 school purposes.

"Parent" has the meaning given to that term under the Illinois School Student Records Act.

"School" means (1) any preschool, public kindergarten, elementary or secondary educational institution, vocational school, special educational facility, or any other elementary or secondary educational agency or institution or (2) any person, agency, or institution that maintains school student records from more than one school. Except as otherwise provided in this Act, "school" includes a private or nonpublic school.

"State Board" means the State Board of Education.

"Student" has the meaning given to that term under the Illinois School Student Records Act.

"Targeted advertising" means presenting advertisements to a student where the advertisement is selected based on information obtained or inferred from that student's online behavior, usage of applications, or covered information. The term 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 ads.

(Source: P.A. 100-315, eff. 8-24-17; 101-516, eff. 7-1-21.)

(105 ILCS 85/10)

Sec. 10. Operator prohibitions. An operator shall not knowingly do any of the following:

(1) Engage in targeted advertising on the operator's site, service, ~~or~~ application, or model or target advertising on any other site, service, ~~or~~ application, or model 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, or model for K through 12 school purposes.

(2) Use information, including persistent unique identifiers, created or gathered by the operator's site, service, ~~or~~ application, or model to amass a profile about a student, except in furtherance of K through 12 school purposes. "Amass a profile" does not include the collection and retention of account information that remains under the control of the student, the student's parent, or the school.

(3) Sell or rent a student's information or data, including covered information or any other person's information collected by the operator for K through 12 school purposes. This subdivision (3) does 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 this Act regarding previously acquired student information.

(3.5) Permit artificial intelligence to train on covered information unless for K through 12 school purposes or in furtherance of improving operability and functionality of the operator's service.

(4) Except as otherwise provided in Section 20 of this Act, disclose covered information, unless the disclosure is made for the following purposes:

(A) In furtherance of the K through 12 school purposes of the site, service, ~~or~~ application, or model if the recipient of the covered information disclosed under this clause (A) does not further disclose the information, unless done to allow or improve operability and functionality of the operator's site, service, or application. Improving operability does not include disclosing covered information to any third party to train artificial intelligence that is not for K through 12 school purposes.

(B) To ensure legal and regulatory compliance or take precautions against liability.

(C) To respond to the judicial process.

(D) To protect the safety or integrity of users of the site or others or the security of the site, service, ~~or~~ application, or model.

(E) For a school, educational, or employment purpose requested by the student or the student's

parent, provided that the information is not used or further disclosed for any other purpose.

(F) To a third party if the operator contractually prohibits the third party from using any covered information for any purpose other than providing the contracted service to or on behalf of the operator, prohibits the third party from disclosing any covered information provided by the operator with subsequent third parties, and requires the third party to implement and maintain security procedures and practices as required under Section 15.

Nothing in this Section prohibits the operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application.

(Source: P.A. 100-315, eff. 8-24-17; 101-516, eff. 7-1-21.)

(105 ILCS 85/15)

Sec. 15. Operator duties. An operator shall do the following:

(1) Implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

(2) Delete, within a reasonable time period, a

student's covered information if the school or school district requests deletion of covered information under the control of the school or school district, unless a student or his or her parent consents to the maintenance of the covered information.

An operator's artificial intelligence model shall not train on a student's covered information and retain the training data indefinitely, unless it first:

(A) informs the student or his or her parent in writing that the operator's artificial intelligence model will retain training data indefinitely; and

(B) receives a written consent from the student or his or her parent.

(3) Publicly disclose material information about its collection, use, and disclosure of covered information, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

(4) Except for a nonpublic school, for any operator who seeks to receive from a school, school district, or the State Board in any manner any covered information, enter into a written agreement with the school, school district, or State Board before the covered information may be transferred. The written agreement may be created in electronic form and signed with an electronic or digital signature or may be a click wrap agreement that is used with software licenses, downloaded or online

applications and transactions for educational technologies, or other technologies in which a user must agree to terms and conditions before using the product or service. Any written agreement entered into, amended, or renewed must contain all of the following:

(A) A listing of the categories or types of covered information to be provided to the operator.

(B) A statement of the product or service being provided to the school by the operator.

(C) A statement that, pursuant to the federal Family Educational Rights and Privacy Act of 1974, the operator is acting as a school official with a legitimate educational interest, is performing an institutional service or function for which the school would otherwise use employees, under the direct control of the school, with respect to the use and maintenance of covered information, and is using the covered information only for an authorized purpose and may not re-disclose it to third parties or affiliates, unless otherwise permitted under this Act, without permission from the school or pursuant to court order.

(D) A description of how, if a breach is attributed to the operator, any costs and expenses incurred by the school in investigating and remediating the breach will be allocated between the operator and the school. The costs and expenses may

include, but are not limited to:

(i) providing notification to the parents of those students whose covered information was compromised and to regulatory agencies or other entities as required by law or contract;

(ii) providing credit monitoring to those students whose covered information was exposed in a manner during the breach that a reasonable person would believe that it could impact his or her credit or financial security;

(iii) legal fees, audit costs, fines, and any other fees or damages imposed against the school as a result of the security breach; and

(iv) providing any other notifications or fulfilling any other requirements adopted by the State Board or of any other State or federal laws.

(E) A statement that the operator must delete or transfer to the school all covered information if the information is no longer needed for the purposes of the written agreement and to specify the time period in which the information must be deleted or transferred once the operator is made aware that the information is no longer needed for the purposes of the written agreement.

(F) If the school maintains a website, a statement that the school must publish the written agreement on

the school's website. If the school does not maintain a website, a statement that the school must make the written agreement available for inspection by the general public at its administrative office. If mutually agreed upon by the school and the operator, provisions of the written agreement, other than those under subparagraphs (A), (B), and (C), may be redacted in the copy of the written agreement published on the school's website or made available at its administrative office.

(5) In case of any breach, within the most expedient time possible and without unreasonable delay, but no later than 30 calendar days after the determination that a breach has occurred, notify the school of any breach of the students' covered information.

(6) Except for a nonpublic school, provide to the school a list of any third parties or affiliates to whom the operator is currently disclosing covered information or has disclosed covered information. This list must, at a minimum, be updated and provided to the school by the beginning of each State fiscal year and at the beginning of each calendar year.

(Source: P.A. 100-315, eff. 8-24-17; 101-516, eff. 7-1-21.)

(105 ILCS 85/25)

Sec. 25. Operator actions that are not prohibited. This

Act does not prohibit an operator from doing any of the following:

(1) Using covered information to improve educational products if that information is not associated with an identified student within the operator's site, service, or application or other sites, services, or applications owned by the operator. This paragraph does not include an operator's artificial intelligence model training on a student's covered information and retaining the training data indefinitely unless the operator satisfies the requirement of paragraph (2) of Section 15.

(2) Using covered information that is not associated with an identified student to demonstrate the effectiveness of the operator's products or services, including in their marketing.

(3) Sharing covered information that is not associated with an identified student for the development and improvement of educational sites, services, or applications. This paragraph does not include an operator's artificial intelligence model training on a student's covered information and retaining the training data indefinitely unless the operator satisfies the requirement of paragraph (2) of Section 15.

(4) Using recommendation engines to recommend to a student either of the following:

(A) Additional content relating to an educational,

other learning, or employment opportunity purpose within an online site, service, or application if the recommendation is not determined in whole or in part by payment or other consideration from a third party.

(B) Additional services relating to an educational, other learning, or employment opportunity purpose within an online site, service, or application if the recommendation is not determined in whole or in part by payment or other consideration from a third party.

(5) Responding to a student's request for information or for feedback without the information or response being determined in whole or in part by payment or other consideration from a third party.

(Source: P.A. 100-315, eff. 8-24-17.)