HOUSE OF REPRESENTATIVES
TWENTY-EIGHTH LEGISLATURE, 2016
STATE OF HAWAII

H.B. NO. 2513

A BILL FOR AN ACT

RELATING TO STUDENT PRIVACY WITH RESPECT TO ELECTRONIC DATA.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. The legislature finds that ensuring the privacy of student information held by educational institutions is of the utmost importance. Although the Family Educational Rights and Privacy Act does provide some protections to students and their families, it does not extend far enough, and explicit state laws are necessary to protect the privacy of students at both public and private educational institutions.

SECTION 2. The Hawaii Revised Statutes is amended by adding a new chapter to be appropriately designated and to read as follows:

"CHAPTER

STUDENT PRIVACY WITH RESPECT TO ELECTRONIC DATA

§ -1 Definitions. As used in this chapter:

"Aggregate data" means student-related data collected and reported by an educational institution at the group, cohort, or institutional level that contains no personally identifiable student information.

"De-identified" means having removed or obscured any personally identifiable information from personally identifiable student information in a manner that prevents the unintended disclosure of the identity of the student or information about the student. Information shall not be considered de-identified if it meets the definition of personally identifiable student information.

"Education research" means the systematic gathering of empirical information to advance knowledge, answer questions, identify trends, or improve outcomes within the field of education.

"Educational institution" means:

(1) A private or public school or institution that offers participants, students, or trainees an organized course of study or training that is academic, trade-oriented, or preparatory for gainful employment, as well as school employees acting under the authority or on behalf of an educational institution; or

(2) A public agency authorized to direct or control an entity in paragraph (1).

"Educational record" means an educational record as defined by 20 U.S.C. §1232g(a)(4) on January 1, 2017.

"Elementary school" means the grade levels falling under the definition of "elementary school," as that term is interpreted by state law for purposes of Section 9101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. §7801 et seq.).

"Law enforcement official" means an officer or employee of any agency or authority of the State, or any of its political subdivisions, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law, make arrests, or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

"Location-tracking technology" means any hardware, software, or application that collects or reports data that identifies the geophysical location of a technological device.

"One-to-one device" means a technological device provided to a student pursuant to a one-to-one program.

"One-to-one device provider" means a person or entity that provides a one-to-one device to a student or educational

institution pursuant to a one-to-one program, and includes any business or non-profit entities that share a parent, subsidiary, or sister relationship with the entity that provides the one-to-one device.

"One-to-one program" means any program authorized by an educational institution where a technological device is provided to a student by or through an educational institution for overnight or at-home use.

"Opt-in agreement" means a discrete, verifiable, written, or electronically generated agreement by which, subject to the provisions of this chapter, a student or the student's parent or legal guardian voluntarily grants a school employee, student information system provider, or one-to-one device provider with limited permission to access and interact with a specifically defined set of personally identifiable student information.

"Personal technological device" means a technological device owned, leased, or otherwise lawfully possessed by a student that was not provided pursuant to a one-to-one program.

"Personally identifiable student information" means 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) A photograph, video recording, or audio recording that contains the student's image or voice;

(5) Indirect identifiers, including but not limited to a student's date of birth, place of birth, mother's maiden name, social security number, student number, biometric record, telephone number, credit card account number, insurance account number, financial services account number, customer number, persistent online identifier, email address, social media address, and other electronic address;

(6) Any aggregate or de-identified student data that is capable of being de-aggregated or reconstructed to the point that individual students can be identified; and

(7) Any student data or other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person, who does not have personal knowledge of the relevant

circumstances, to identify a specific student with reasonable certainty.

"School employee" means an individual who is employed by an educational institution, compensated through an annual salary or hourly wage paid by an educational institution, and whose services are primarily rendered at a physical location that is owned or leased by that educational institution. As used in this chapter, individuals with law enforcement or school security responsibilities, including school resource officers, contract or private security companies, security guards, or other law enforcement personnel shall not be considered school employees.

"Student" means any student, participant, or trainee, whether full-time or part-time, in an organized course of study at an educational institution.

"Student data" means data that is collected and stored by an educational institution, or by a person or entity acting on behalf of that institution, and included in a student's educational record.

"Student information system" means a software application or cloud-based service that allows an educational institution to

enter, maintain, manage, or retrieve student data or personally identifiable student information, including applications that track or share personally identifiable student information in real time.

"Student information system provider" means an entity that sells, leases, provides, operates, or maintains a student information system for the benefit of an educational institution.

"Technological device" means 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.

§ -2 Student information systems; requirements. Any contract or other agreement between an educational institution and a student information system provider pursuant to which the student information system provider sells, leases, provides, operates, or maintains a student information system for the benefit of the educational institution shall:

(1) Expressly authorize and require the student information service provider to:

(A) Establish, implement and maintain appropriate security measures, consistent with best current practices, to protect the student data and personally identifiable student information that the student information system provider creates, sends, receives, stores, and transmits in conjunction with the operation of the student information system;

(B) Acknowledge that no data stored on the student information system is the property of the student information system provider;

(C) Establish and implement policies and procedures for responding to data breaches involving the unauthorized acquisition of or access to any personally identifiable student information on the student information system. Such policies and procedures shall, at a minimum:

(i) Require notice be provided by the student information system provider to any and all affected parties, including educational institutions, students, and students'

parents and legal guardians, within thirty days of the discovery of the breach;

(ii) Require the notice to include a description of the categories of sensitive personally identifiable student information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(iii) Require the notice to provide a procedure by which affected parties may learn what types of sensitive personally identifiable student information that the student information system provider maintained about the affected individual; and

(iv) Satisfy all other applicable breach notification standards established under state or federal law;

(D) Permanently delete all data stored on the student information system, and destroy all non-digital records containing any personally identifiable student information retrieved from the student

information system, within ninety days of the termination of the student information system provider's contact with the educational institution, except where the student information system provider and the individual or individuals authorized to sign a valid opt-in agreement pursuant to section -3(b) mutually agree that the student information system provider will retain specifically identified data or non-digital records for the student's benefit; provided that prior to deletion, if requested by the educational institution, the terminated student information service provider shall transfer a designated portion or all of the data stored on the student information system to another designated student information system provider at the educational institution's expense; and

(E) Comply with all the applicable obligations and restrictions established for student information system providers in this chapter;

(2) Expressly prohibit the student information system provider from:

(A) Analyzing, interacting with, sharing, or transferring any student data or personally identifiable student information that the educational institution enters into or otherwise provides to the student information system, unless:

(i) Permission to do so has been granted, pursuant to a opt-in agreement under section -3;

(ii) The student information system provider analyzes or interacts with the student data or personally identifiable student information to meet a contractual obligation to the educational institution and any analysis of or interaction with the data or information is limited to meeting that contractual obligation;

(iii) The student information system provider analyzes or interacts with the student data

or personally identifiable student information in response to a specific request made by an educational institution and any data or information produced as a result of the analysis or interaction is limited to the educational purpose for which it was sought;

(iv) The educational institution determines, and documents in writing, that sharing specific student data or personally identifiable student information is necessary to safeguard students' health or safety while students are traveling to or from the educational institution, are on the educational institution's property, or are participating in an event or activity supervised by the educational institution; or

(v) At the request of the educational institution, the student information system provider de-identifies or aggregates student

data or personally identifiable student information for the purpose of enabling the educational institution to comply with federal, state, or local reporting and data-sharing requirements, or education research;

(vi) The data is accessed by the student information system provider for the exclusive purpose of testing and improving the value and performance of its student information system for the benefit of the educational institution;

(vii) Where data is accessed to test and improve student information system value and performance, any copied data shall be permanently deleted within sixty days of the date the copy was created and any data analysis that contains personally identifiable student information shall be permanently deleted within sixty days of the date that the analysis was created;

(B) Selling any student data or personally identifiable student information stored on or retrieved from the student information system unless it is sold as part of a sale or merger of the entirety of the student information system provider's business. Upon such a sale or merger, the provisions of this chapter, and any relevant contracts or agreements, shall apply fully to the new purchasing or controlling person or entity;

(C) Using any student data or personally identifiable student information stored on or retrieved from the student information system to inform, influence, or guide marketing or advertising efforts directed at a student, a student's parent or legal guardian, or a school employee, except pursuant to a valid opt-in agreement pursuant to section -3;

(D) Using any student data or personally identifiable student information stored on or retrieved from the student information system to develop, in full or in part, a profile of a student or group

of students for any commercial or other non-educational purposes.

§ -3 Opt-in agreements; student information system. (a) A valid opt-in agreement shall identify, with specificity:

(1) The precise subset of personally identifiable student information in the student information system (e.g., student attendance records, student disciplinary records) for which the student information system provider is being granted authority to access, analyze, interact with, share, or transfer;

(2) The name of the student information system provider to whom the authority to access, analyze, interact with, share, or transfer personally identifiable student information in the student information system is being granted;

(3) The educational purpose for which the authority to access, analyze, interact with, share, or transfer personally identifiable student information is being granted; and

(4) The individual student to whom the opt-in agreement applies.

(b) An opt-in agreement shall be valid only if it has been signed by:

(1) The student's parent or legal guardian, if the student is in elementary school;

(2) The student and the student's parent or legal guardian, if the student has advanced beyond elementary school but has not yet reached the age of majority; or

(3) The student alone, if the student has reached the age of majority.

(c) A valid opt-in agreement may authorize a student information system provider to share or transfer personally identifiable student information to another person or entity only if:

(1) The purpose of the transfer of the personally identifiable student information is to benefit:

(A) The operational, administrative, analytical, or educational functions of the educational institution, including education research; or

(B) The student's education;

(2) The subset of personally identifiable student information to be shared or transferred is identified with specificity in the opt-in agreement;

(3) The person or entity with or to whom the personally identifiable student information is being shared or transferred is identified with specificity in the opt-in agreement;

(4) The benefit to the educational institution or student is identified with specificity in the opt-in agreement; and

(5) For each student, a record of what specific personally identifiable student information pertaining to that student was shared or transferred, when it was shared or transferred, and with or to whom it was shared or transferred is appended to the student's record.

(d) Any person or entity that accesses or takes possession of any student data or personally identifiable student information pursuant to section -2(a)(2)(i) or section -2(a)(2)(B) shall be subject to the same restrictions and obligations under this section as the student information system

provider from which the student data or personally identifiable student information was obtained.

(e) An opt-in agreement shall not be valid if it grants general authority to access, analyze, interact with, share, or transfer a student's personally identifiable student information in a student information system.

(f) Except as authorized in this section, no student information system provider, school employee, or other person or entity who receives personally identifiable student information, directly or indirectly, from a student information system pursuant to an opt-in agreement may share, sell, or otherwise transfer such information to another person or entity.

(g) An opt-in agreement may be revoked at any time, upon written notice to an educational institution, by the person or persons eligible to authorize an opt-in agreement pursuant to subsection (b). Within thirty days of such a revocation, the educational institution shall provide notice to the student information system provider.

(h) A student information system provider that accesses, analyzes, interacts with, shares, or transfers personally identifiable student information to another person or entity

shall bear the burden of proving that it acted pursuant to a valid opt-in agreement.

(i) No educational benefit may be withheld from, or punitive measure taken against, a student or the student's parent or legal guardian based in whole or in part upon a decision not to sign, or to revoke, an opt-in agreement.

§ -4 School employees. (a) Subject to written authorization from the educational institution, school employees may access and interact with student data and personally identifiable student information on a student information system in furtherance of their professional duties.

(b) No school employee may receive authorization to access and interact with student data or personally identifiable student information on a student information system until the employee has received adequate training to ensure the school employee's understanding and compliance with the provisions of this chapter.

(c) School employees may not sell, share, or otherwise transfer student data or personally identifiable student information to another person or entity, except:

(1) Where specifically authorized to do so pursuant to this chapter;

(2) With the educational institution that employs the school employee;

(3) With another school employee who is eligible to access such information pursuant to subsection (a); and

(4) Where:

(A) The school employee is a teacher;

(B) The teacher is transferring student data to a software application for classroom recordkeeping or management purposes only;

(C) Any third parties with access to the software application are expressly prohibited from reviewing or interacting with the transferred data; and

(D) Any data transferred to the software application by the teacher is deleted by the teacher within forty-five days of such time as it is no longer being actively used for classroom recordkeeping or management purposes.

§ -5 Authority to review student data and personally identifiable student information. (a) Upon written request to an educational institution, a student's parent or legal guardian may inspect and review the student's student data and personally identifiable student information that is stored on a student information system. Educational institutions shall afford parents and legal guardians a reasonable and fair opportunity to request corrections to or seek removal of inaccurate data.

(b) The right of a student's parent or legal guardian to review the student's student data and personally identifiable student information shall not apply where:

(1) Such information was supplied by the student to the educational institution and there is a reasonable likelihood the disclosure of such information would cause a threat to the student's health or safety; or

(2) Access to particularly specified information has been waived by the student or the student's parent or legal guardian.

(c) When a student reaches the age of majority, the rights granted to a student's parent or legal guardian pursuant to this section shall terminate and instead shall vest with the student.

(d) An educational institution shall establish appropriate procedures for:

(1) Reviewing and responding to requests made pursuant to this section within thirty days of receipt of the request; and

(2) Requesting and receiving a fair hearing in the event a requested correction is denied.

§ -6 Treatment of student data and personally identifiable student information. (a) One year after a student's graduation, withdrawal, or expulsion from an educational institution, all student data and personally identifiable student information related to that student that is stored in a student information system shall be deleted, except for:

(1) A student's name and social security number;

(2) A student's transcript, graduation record, letters of recommendation, and other information required by an institution of higher education for an application for admission or by a potential employer for an application for employment;

(3) Student data and personally identifiable student information that is the subject of an ongoing disciplinary, administrative, or judicial action or proceeding;

(4) De-identified student data that is being retained at the request of the educational institution for the purpose of education research or analysis; and

(5) Student data or personally identifiable student information where its retention is otherwise required by law or a judicial order or warrant.

(b) Within one hundred eighty days of receiving notification, pursuant to subsection (c), of a student's graduation, withdrawal, or expulsion from an educational institution, all physical or digital copies of any student data and personally identifiable student information related to the student that was obtained from a student information system and is in the possession or under the control of a student information service provider or other third party shall be deleted or destroyed, except for:

(1) Student data and personally identifiable student information that is the subject of an ongoing

disciplinary, administrative, or judicial action or proceeding;

(2) Aggregated or de-identified student data obtained for the purpose of education research;

(3) Student data or personally identifiable student information where its retention is otherwise required by law or a judicial order or warrant; and

(4) Specifically identified student data or personally identifiable student information, where:

(A) Its retention is requested by the person authorized to sign a valid opt-in agreement pursuant to section -3(b); and

(B) The student information service provider and educational institution voluntarily consent to its retention.

(c) Within ninety days of a student's graduation, withdrawal, or expulsion from an educational institution, notice of such shall be provided by the educational institution to the student information service provider, which shall in turn notify any third parties with whom the student information service

provider shared the student's student data or personally identifiable student information.

(d) No person or entity, other than an educational institution, school employee, or student information service provider, except as provided for in this section, shall be granted access to review or interact with a student information system and the data thereon, unless otherwise authorized to do so by law, pursuant to a judicial warrant, or as part of an audit initiated by an educational institution.

(e) This section shall not be construed to:

(1) Prohibit an educational institution from providing directory information to a vendor for the express purpose of providing photography services, class ring services, yearbook or student publication publishing services, memorabilia services, or similar services, provided the vendor agrees in writing:

(A) Not to sell or transfer the data to any other persons or entities;

(B) To use the data solely for the express purpose for which it was provided; and

(C) To destroy the data upon completion of its use for the express purpose for which it was provided; and

(2) Supersede or otherwise limit any laws that provide enhanced privacy protections to students or further restrict access to their educational records or personally identifiable student information.

§ -7 **One-to-one programs.** (a) Where an educational institution or one-to-one device provider provides a student with a technological device pursuant to a one-to-one program, no school employee or one-to-one device provider, or an agent thereof, may access or track such a device or the activity or data thereupon, either remotely or in person, except in accordance with the provisions of this section.

(b) No school employee or one-to-one device provider, or an agent thereof, may access any data entered into, stored upon, or sent or received by a student's one-to-one device, including but not limited to its browser, key stroke history, or location history, nor may such data be analyzed, interacted with, shared, or transferred unless:

(1) The data being collected is not personally identifiable student information;

(2) The data is being accessed by or on behalf of school employee who:

(A) Is the student's teacher;

(B) Is receiving or reviewing the information for an educational purpose consistent with the teacher's professional duties; and

(C) Does not use the information, or permit any other person or entity to use the information, for any other purpose;

(3) A school employee or one-to-one device provider or an agent thereof has been authorized to access specific personally identifiable student information pursuant to an opt-in agreement pursuant to section -8;

(4) A school employee has a reasonable suspicion that the student has violated or is violating an educational institution's policy and that data on the one-to-one device contains evidence of the suspected violation, subject to the following limitations:

(A) Prior to searching a student's one-to-one device based on reasonable individualized suspicion, the school employee shall document the reasonable individualized suspicion and notify the student and the student's parent or legal guardian, as applicable, of the suspected violation and what data will be accessed in searching for evidence of the violation;

(i) Subject to any other law, an educational institution may seize a student's personal technological device to prevent data deletion pending notification pursuant to subsection (b)(2); provided that the pre-notification seizure period does not exceed forty-eight hours; and

(ii) Subject to any other law, an educational institution may seize a student's one-to-one device; provided that the one-to-one device is stored securely on the educational institution's property and is not accessed during the pre-notification seizure period;

(B) Searches of a student's device based upon a reasonable individualized suspicion that an educational institution's policy has been violated shall be strictly limited to finding evidence of the suspected policy violation and shall immediately cease upon finding sufficient evidence of the suspected violation. It shall be a violation of this subsection to copy, share, or transfer any data, or any information thereabout, that is unrelated to the specific suspected violation that prompted the search of the one-to-one device; and

(C) Where a student is suspected of illegal conduct, no search of the one-to-one device may occur unless a judicial warrant has been secured in accordance with paragraph (5), even if the student is also suspected of a related or unrelated violation of the educational institution's policy;

(5) A school employee or law enforcement official reasonably suspects that the student has engaged or is

engaging in illegal conduct, reasonably suspects data on the one-to-one device contains evidence of the suspected illegal conduct, and has secured a judicial warrant for a search of the device;

(6) Doing so is necessary to update or upgrade the device's software, or protect the device from cyber-threats, and access is limited to that purpose;

(7) Doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose; provided that within seventy-two hours of accessing a one-to-one device's data 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 with a written description of the precise threat that prompted the access and what data was accessed; or

(8) The information sent from the device is posted on a website that:

(A) Is accessible by the general public; or

(B) Is accessible by a specific school employee who was granted permission by the student to view the content.

(c) No school employee or one-to-one device provider, or an agent thereof, may use a student's one-to-one device's location-tracking technology to track a device's real-time or historical location, unless:

(1) Such use is ordered pursuant to a judicial warrant;

(2) The student to whom the device was provided, or the student's parent or legal guardian, has notified a school employee or law enforcement official that the device is missing or stolen; or

(3) Doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose; provided that within seventy-two hours of accessing a one-to-one device's location-tracking technology 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 precise threat that prompted the access and what data and features were accessed.

(d) No school employee or one-to-one device provider, or an agent thereof, may activate or access any audio or video receiving, transmitting, or recording functions on a student's one-to-one device, unless:

(1) A student initiates a video chat or audio chat with the school employee or one-to-one device provider;

(2) The activation or access is ordered pursuant to a judicial warrant; or

(3) Doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose; provided that within seventy-two hours of accessing a one-to-one device's audio or video receiving, transmitting, or recording functions 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 precise threat that prompted the access and what data and features were accessed.

(e) No school employee, or an agent thereof, may use a one-to-one device, or require a student to use a one-to-one device in the employee or agent's presence, in order to view or gain access to a student's password-protected software, website accounts, or applications, except where:

(1) The school employee is a teacher;

(2) The student is enrolled in and participating in a class taught by the teacher; and

(3) The viewing of the one-to-one device relates exclusively to an educational purpose.

(f) No one-to-one device provider, or an agent thereof, may use any student data or personally identifiable student information stored on or retrieved from a one-to-one device to:

(1) Inform, influence, or direct marketing or advertising efforts directed at a student, a student's parent or legal guardian, or a school employee, except pursuant to a valid opt-in agreement; or

(2) Develop, in full or in part, a student profile for any commercial or other non-educational purpose.

(g) Notwithstanding any other provision of this section, no school employee may supervise, direct, or participate in a one-to-one program, or access any one-to-one device or data thereupon, until the employee has received adequate training to ensure the school employee's understanding of and compliance with this section.

(h) No personally identifiable student information obtained or received from a one-to-one device by a school employee or one-to-one device provider may be sold, shared, or otherwise transferred to another person or entity, except:

(1) To another school employee who has satisfied the requirements of subsection (i) and is accessing the information in furtherance of the employee's professional duties; or

(2) Where a one-to-one device provider has been authorized to do so pursuant to an opt-in agreement pursuant to section -8.

§ -8 Opt-in agreements; one-to-one device. (a) A valid opt-in agreement shall identify, with specificity:

(1) The precise subset of personally identifiable student information on the one-to-one device to which the

authority to access, analyze, and interact is being granted;

(2) The name of the school employee or one-to-one device provider to whom the authority to access, analyze, and interact with the personally identifiable student information on the one-to-one device is being granted;

(3) The educational purpose for which the school employee or one-to-one device provider is being granted the authority to access, analyze, and interact with the personally identifiable student information on the one-to-one device; and

(4) The individual student to whom the opt-in agreement applies.

(b) An opt-in agreement shall be valid only if it has been signed by:

(1) The student's parent or legal guardian, if the student is in elementary school;

(2) The student and the student's parent or legal guardian, if the student has advanced beyond elementary school but has not yet reached the age of majority; or

(3) The student alone, if the student has reached the age of majority.

(c) An opt-in agreement shall not be valid if it actually or effectively grants a one-to-one device provider:

(1) General authority to access a student's one-to-one device; or

(2) The authority to collect all the personally identifiable student information that is generated by or used in connection with a specific program or application.

(d) An opt-in agreement may be revoked at any time, upon written notice to an educational institution, by the person eligible to authorize an opt-in agreement under subsection (b). Within thirty days of such a revocation, the educational institution shall notify any affected third parties.

(e) A one-to-one device provider that accesses, analyzes, and interacts with personally identifiable student information on a one-to-one device shall bear the burden of proving that it acted pursuant to a valid opt-in agreement.

(f) No one-to-one device program offered to an educational institution or its students may be conditioned upon the

exclusive use of any software, application, website, or internet-based service sold or provided by the one-to-one device provider.

(g) No one-to-one device or related educational benefit may be withheld from, or punitive measure taken against, a student or the student's parent or legal guardian:

(1) Based in whole or in part upon a decision not to sign, or to revoke, an opt-in agreement; or

(2) Based in whole or in part upon a student's refusal to open, close, or maintain an email or other electronic communications or social media account with a specific service provider.

(h) A one-to-one device provider shall violate subsection (g)(1) if it conditions the offer, provision, or receipt of a one-to-one device upon a student's or the student's parent's or legal guardian's agreement to provide access to personally identifiable student information.

§ -9 Protection of student data. (a) No school employee or one-to-one device provider, or an agent thereof, who receives or collects personally identifiable student information from a one-to-one device may share, sell, or otherwise transfer

such data to another person or entity unless, in the case of a one-to-one device provider, such information is sold as part of a sale or merger of the entirety of the one-to-one device provider's business.

(b) Any entity that purchases personally identifiable student information shall be subject to the same restrictions and obligations as the one-to-one device provider from which the personally identifiable student information was obtained.

(c) No person or entity, other than an educational institution, school employee, or one-to-one device provider subject to the limitations set forth in this section, shall be provided direct access to review or interact with a one-to-one device and the data thereon, unless otherwise authorized to do so by law, pursuant to a judicial warrant, or upon the express permission of the student to whom the one-to-one device is issued.

(d) When a one-to-one device is permanently returned by a student, the educational institution or one-to-one device provider who provided it shall, without otherwise accessing the data on the one-to-one device, fully delete all the data stored

on the device and return the device to its default factory settings.

(e) The provisions of this section that relate to the collection and use of personally identifiable student information shall not apply to personally identifiable student information collected by a one-to-one provider from a software program, website, or application that was:

(1) Not pre-loaded on the one-to-one device;

(2) Not the target of a link that was pre-loaded on the one-to-one device; and

(3) Not promoted, marketed, or advertised in connection with the issuance of the one-to-one device.

§ -10 Personal technological devices. (a) No school employee may access, or compel a student to produce, display, share, or provide access to, any data or other content entered into, stored upon, or accessible from a student's personal technological device, even where the personal technological device is being carried or used in violation of an educational institution's policy.

(b) Notwithstanding subsection (a), a school employee may search a student's personal technological device, if the school

employee has a reasonable suspicion that a student has violated or is violating an educational institution's policy and that the student's personal technological device contains evidence of the suspected violation. In such cases, the school employee may search the student's personal technological device if the student's personal technological device is located on the property of the educational institution. Prior to searching a student's personal technological device, the school employee shall:

(1) Document the reasonable individualized suspicion giving rise to the need for the search; and

(2) Notify the student and the student's parent or legal guardian, as applicable, of the suspected violation and what data will be accessed in searching for evidence of the violation.

The search shall be strictly limited to finding evidence of the suspected policy violation, and the school employee shall immediately cease to search the student's personal technological device upon finding sufficient evidence of the suspected violation.

(c) Subject to any other law, an educational institution may seize a student's personal technological device to prevent data deletion pending notification pursuant to subsection (b)(2); provided that:

(1) The pre-notification seizure period does not exceed forty-eight hours; and

(2) The personal technological device is stored securely on the educational institution's property and is not accessed during the pre-notification seizure period.

(d) It shall be a violation of this section to copy, share, or transfer any data, or any information thereabout, that is unrelated to the specific suspected violation that prompted the search of the student's personal technological device pursuant to subsection (b).

(e) Notwithstanding subsection (a), a school employee or law enforcement official may search a student's personal technological device, if doing so is necessary in response to an imminent threat to life or safety. Within seventy-two hours of accessing a student's personal technological 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 precise threat that prompted the access and what data was accessed.

(f) Notwithstanding subsection (b), where a student is suspected of illegal conduct, no search of the student's personal technological device may occur unless a judicial warrant authorizing a law enforcement official to search the student's personal technological device has been secured, even if the student is also suspected of a related or unrelated violation of an educational institution's policy.

§ -11 Limitations on use of evidence or information. Evidence or information obtained or collected in violation of this chapter shall not be admissible in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing.

§ -12 Penalties. (a) Any person or entity who violates this chapter shall be subject to legal action for damages or equitable relief, to be brought by any other individual claiming a violation of this chapter has injured the individual's person or reputation. An individual so injured shall be entitled to

actual damages, including mental pain and suffering endured on account of a violation of this chapter; reasonable attorney's fees; and other costs of litigation.

(b) Any school employee who violates this chapter, or any rule adopted pursuant to this chapter, may be subject to disciplinary proceedings and punishment. For school employees who are represented under the terms of a collective bargaining agreement, this chapter shall prevail, except where it conflicts with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit."

SECTION 3. If any provision of this Act, or the application thereof to any person or circumstance, is held invalid, the invalidity does not affect other provisions or applications of the Act that can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

SECTION 4. This Act shall take effect on January 1, 2017.

INTRODUCED BY: _____

H.B. NO. 2513

JAN 26 2016

H.B. NO. 2513

Report Title:
Student Privacy; Electronic Data

Description:
Protects student privacy with respect to electronic data.

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.