HOUSE BILL NO. 690

INTRODUCED BY K. SULLIVAN

A BILL FOR AN ACT ENTITLED: “AN ACT GENERALLY REVISING PUPIL DATA PRIVACY PROTECTIONS; LIMITING THE USE OF FACIAL RECOGNITION TECHNOLOGY BY A SCHOOL DISTRICT; REQUIRING A VENDOR PROVIDING FACIAL RECOGNITION TECHNOLOGY TO A SCHOOL DISTRICT TO DELETE FACIAL BIOMETRIC DATA IMMEDIATELY ON TERMINATION OF THE CONTRACT WITH THE SCHOOL DISTRICT; CLARIFYING THAT PROTECTED INFORMATION INCLUDES INFORMATION CREATED THROUGH THE USE OF FACIAL RECOGNITION TECHNOLOGY; REQUIRING CONTRACTUAL OBLIGATIONS FOR THIRD PARTY OPERATORS TO COMPLY WITH THE MONTANA PUPIL ONLINE PERSONAL INFORMATION PROTECTION ACT; REQUIRING PROVISION OF NOTICE OF SURVEILLANCE ON SCHOOL DISTRICT PROPERTY; PROVIDING DEFINITIONS; AMENDING SECTIONS 20-7-1324, 20-7-1326, AND 45-8-213, MCA; AND PROVIDING AN IMMEDIATE EFFECTIVE DATE AND AN APPLICABILITY DATE.”

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

NEW SECTION. **Section 1. Facial recognition technology -- limited uses -- vendor requirements.** (1) A school district may use facial recognition technology in a public school only for the following purposes:

(a) to investigate a crime that was committed at the school;

(b) when an injury occurs on campus in order to determine the cause of the injury;

(c) to monitor the entry and exit of individuals on the campus; or

(d) to locate a dangerous or suspicious person on the campus.

(2) A school district may not use facial recognition technology for any purpose beyond the safety of students, employees, and other people at school.

(3) A vendor, including an operator or a third party as those terms are defined in 20-7-1324, that contracts with a school district to provide facial recognition technology may use facial biometric data only for the

purposes of assisting a school district with the allowable uses under subsection (1).

(4) (a) A vendor may not use facial biometric data or any other data collected through facial recognition technology for marketing, product demonstrations, or any other purpose.

(b) A vendor may not sell, lease, trade, or otherwise share facial biometric data or other data collected through facial recognition technology. This prohibition applies regardless of whether the data is deidentified information as defined in 20-7-1324.

(5) A vendor shall delete all facial biometric data and other data collected through facial recognition technology immediately on termination of the contract between the vendor and the school district.

(6) For the purposes of this section, the following definitions apply:

(a) "Facial biometric data" means data derived from a measurement, pattern, contour, or other characteristic of an individual's face, either directly or from an image.

(b) (i) "Facial identification" means a computer system that, for the purpose of attempting to determine the identity of an unknown individual, uses an algorithm to compare the facial biometric data of an unknown individual derived from a photograph, video, or image to a database of photographs or images and associated facial biometric data to identify potential matches.

(ii) The term does not include:

(A) a system used specifically to protect against unauthorized access to a particular location or an electronic device; or

(B) a system an individual uses for the individual's private purposes.

(c) "Facial recognition technology" means the use of facial identification or facial verification.

(d) "Facial verification" means the automated process of comparing an image or facial biometric data of a known individual to an image database or to government documentation containing an image of the known individual to identify a potential match in pursuit of the individual's identity.

(e) "Public school" or "school" means a building, grounds, or property of a public elementary or secondary school.

Section 2. Section 20-7-1324, MCA, is amended to read:

"**20-7-1324. Definitions.** As used in 20-7-1323 through 20-7-1326, the following definitions apply:

(1) "Deidentified information" means information that cannot be used to identify an individual pupil.

(2) "K-12 online application" means an internet website, online service, cloud computing service, online application, or mobile application that is used primarily for K-12 school purposes and that was designed and is marketed for K-12 school purposes.

(3) "K-12 school purposes" means activities that customarily take place at the direction of a school, teacher, or school district or aid in the administration of school activities, including but not limited to instruction in the classroom or at home, administrative activities, and collaboration between pupils, school personnel, or parents, or that are for the use and benefit of a school.

(4) "Online privacy protections" means the school district policies and contractual provisions required pursuant to 20-7-1326.

~~(4)~~(5) "Operator" means the operator of a K-12 online application who is an employee or a third party of a school district who knows or reasonably should know that the application is used primarily for K-12 school purposes.

~~(5)~~(6) (a) "Protected information" means personally identifiable information or materials, in any media or format, that describes or otherwise identifies a pupil and that is:

(i) created or provided by a pupil, or the pupil's parent or legal guardian, to an operator in the course of the pupil's, parent's, or legal guardian's use of the operator's K-12 online application;

(ii) created or provided by an employee or agent of a school district to an operator in the course of the employee's or agent's use of the operator's K-12 online application; or

(iii) gathered by an operator through the operator's K-12 online application.

(b) The term includes any information meeting the definition under subsection (6)(a), including but ~~is~~ not limited to:

(i) information in the pupil's educational record or e-mail messages;

(ii) first and last name, home address, telephone number, e-mail address, or other information that allows physical or online contact;

(iii) discipline records, test results, special education data, juvenile dependency records, grades, or evaluations;

(iv) criminal, medical, or health records;

(v) social security number;

(vi) biometric information;

(vii) disability;

(viii) socioeconomic information;

(ix) food purchases;

(x) political affiliation;

(xi) religious information; ~~or~~

(xii) text messages, documents, pupil identifiers, search activity, photos, voice recordings, or geolocation information; or

(xiii) information created through the use of facial recognition technology.

~~(6)~~(7) (a) "Pupil records" means:

(i) any protected information directly related to a pupil that is maintained by a school district through electronic means, including cloud-based services and digital software that can be used to access, store, and use protected information; or

(ii) any information acquired directly from a pupil through the use of instructional software or applications assigned to the pupil by a teacher or other school district employee.

(b) The term does not include deidentified information, including aggregated deidentified information used:

(i) by a third party to improve educational products for adaptive learning purposes, to ensure school and student safety and security, and for customizing pupil learning;

(ii) to demonstrate the effectiveness of a third party's products in the marketing of those products; or

(iii) for the development and improvement of educational sites, services, or applications.

~~(7)~~(8) (a) "Pupil-generated content" means materials created by a pupil, including but not limited to essays, research reports, portfolios, creative writing, music or other audio files, photographs, and account information that enables ongoing ownership of pupil content.

(b) The term does not include pupil responses to a standardized assessment for which pupil possession and control would jeopardize the validity and reliability of that assessment.

~~(8)~~(9) "Third party" refers to a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records."

Section 3. Section 20-7-1326, MCA, is amended to read:

"**20-7-1326. Pupil records -- online privacy protections.** (1) ~~A school district may, pursuant to a policy adopted by its trustees, enter into a contract with a third party to:~~

~~(a) provide services, including cloud-based services, for the digital storage, management, and retrieval of pupil records; or~~

~~(b) provide digital educational software that authorizes a third-party provider of digital educational software to access, store, and use pupil records in accordance with the contractual provisions listed in subsection (2).~~ Online privacy protections specified under this section must be implemented by any school district or operator that uses a K-12 online application for K-12 purposes to collect, track, or use protected information or pupil records, including pupil-generated content.

(2) ~~A school district that enters into a contract with a third party for purposes of subsection (1) shall ensure the contract contains~~ A school district shall adopt a policy requiring online privacy protections through compliance directives that apply to employee operators and through contractual provisions that apply to third party operators that include all of the following:

(a) a statement that pupil records continue to be the property of and under the control of the school district;

(b) notwithstanding subsection (2)(a), a description of the means by which pupils may retain possession and control of their own pupil-generated content, if applicable, including options by which a pupil may transfer pupil-generated content to a personal account;

(c) a prohibition against ~~the third party for~~ an operator using any information in pupil records for any purpose other than those required or specifically permitted by the policy or contract;

(d) a description of the procedures by which a parent, legal guardian, or eligible pupil may review personally identifiable information in the pupil's records and correct erroneous information;

(e) a description of the actions the ~~third party~~ operator of a K-12 online application will take, including the designation and training of responsible individuals, to ensure the security and confidentiality of

pupil records. Compliance with this requirement does not, in itself, absolve the ~~third party~~ operator of liability in the event of an unauthorized disclosure of pupil records.

(f) a description of the procedures for notifying the affected parent, legal guardian, or pupil if 18 years of age or older in the event of an unauthorized disclosure of the pupil's records;

(g) a ~~certification~~ requirement that pupil records will not be retained or available to ~~the~~ a third party operator ~~upon~~ on completion of the terms of the contract and a description of how that ~~certification~~ requirement will be enforced. This requirement does not apply to pupil-generated content if a pupil chooses to establish or maintain an account with the third party operator for the purpose of storing that content pursuant to subsection (2)(b).

(h) a description of how the school district and the third party will jointly ensure compliance with the federal Family Educational Rights and Privacy Act (20 U.S.C. 1232g); and

(i) a prohibition against the third party operator using personally identifiable information in pupil records to engage in targeted advertising.

(3) A school district may satisfy its obligation to execute a contract with the third party operator of a K-12 online application by using a model contract approved by a public or private consortium that uses binding standards of privacy that meet or exceed the requirements of this section.

~~(3)~~(4) In addition to any other penalties, a contract that fails to comply with the requirements of this section is void if, ~~upon~~ on notice and a ~~reasonable~~ 30-day opportunity to cure, the noncompliant party fails to come into compliance and cure any defect. ~~Written~~ A school district shall provide notice of noncompliance ~~may be provided by any party to the contract~~ and notice of a 30-day opportunity to cure within 10 days following the discovery of the noncompliance. All ~~parties~~ third party operators of a K-12 online application subject to a contract voided under this ~~subdivision~~ section shall return all pupil records, protected information, pupil-generated content, and deidentified information in their possession to the school district on expiration of the 30-day opportunity to cure.

~~(4)~~(5) If the provisions of this section are in conflict with the terms of a contract in effect before ~~May 7, 2019~~ [the effective date of this act], the provisions of this section do not apply to the school district or the third party subject to that agreement until the expiration, amendment, or renewal of the agreement.

~~(5)~~(6) Nothing in this section may be construed to impose liability on a third party for content provided

by any other third party.

(7) The office of public instruction and the department of administration shall coordinate to verify compliance of third party operators and school districts with the contract requirements under this section."

Section 4. Section 45-8-213, MCA, is amended to read:

"**45-8-213. Privacy in communications.** (1) Except as provided in 69-6-104, a person commits the offense of violating privacy in communications if the person knowingly or purposely:

(a) with the purpose to terrify, intimidate, threaten, harass, or injure, communicates with a person by electronic communication and threatens to inflict injury or physical harm to the person or property of the person or makes repeated use of obscene, lewd, or profane language or repeated lewd or lascivious suggestions;

(b) uses an electronic communication to attempt to extort money or any other thing of value from a person or to disturb by repeated communications the peace, quiet, or right of privacy of a person at the place where the communications are received;

(c) records or causes to be recorded a conversation by use of a hidden electronic or mechanical device that reproduces a human conversation without the knowledge of all parties to the conversation; or

(d) with the purpose to terrify, intimidate, threaten, harass, or injure, publishes or distributes printed or electronic photographs, pictures, images, or films of an identifiable person without the consent of the person depicted that show:

(i) the visible genitals, anus, buttocks, or female breast if the nipple is exposed; or

(ii) the person depicted engaged in a real or simulated sexual act.

(2) (a) Subsection (1)(c) does not apply to:

(i) elected or appointed public officials or to public employees when the transcription or recording is done in the performance of official duty;

(ii) persons speaking at public meetings;

(iii) persons given warning of the transcription or recording. If one person provides the warning, either party may record.

(iv) a health care facility, as defined in 50-5-101, or a government agency that deals with health

care if the recording is of a health care emergency telephone communication made to the facility or agency. ; or

(v) the use of audio or video surveillance or facial recognition technology that complies with the requirements of 20-7-1326 by a school district board of trustees pursuant to 20-3-324 to protect school and student safety and security and the health, welfare, and safety of all students, staff, and visitors to district property and to safeguard school buildings, grounds, buses, and equipment. A notice must be posted at the main entrance of all district buildings and on all buses indicating the district's use of audio or video surveillance or facial recognition technology.

(b) Subsection (1)(d) does not apply to:

(i) images involving the voluntary exposure of a person's genitals or intimate parts in public or commercial settings;

(ii) disclosures made in the public interest, including but not limited to the reporting of unlawful conduct;

(iii) disclosures made in the course of performing duties related to law enforcement, including reporting to authorities, criminal or news reporting, legal proceedings, or medical treatment; or

(iv) disclosures concerning historic, artistic, scientific, or educational materials.

(3) Except as provided in 69-6-104, a person commits the offense of violating privacy in communications if the person purposely intercepts an electronic communication. This subsection does not apply to elected or appointed public officials or to public employees when the interception is done in the performance of official duty or to persons given warning of the interception.

(4) (a) A person convicted of the offense of violating privacy in communications shall be fined an amount not to exceed $500 or be imprisoned in the county jail for a term not to exceed 6 months, or both.

(b) On a second conviction of subsection (1)(a), (1)(b), or (1)(d), a person shall be imprisoned in the county jail for a term not to exceed 1 year or be fined an amount not to exceed $1,000, or both.

(c) On a third or subsequent conviction of subsection (1)(a), (1)(b), or (1)(d), a person shall be imprisoned in the state prison for a term not to exceed 5 years or be fined an amount not to exceed $10,000, or both.

(5) Nothing in this section may be construed to impose liability on an interactive computer service for content provided by another person.

(6) As used in this section, the following definitions apply:

(a) "Electronic communication" means any transfer between persons of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system.

(b) "Interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet and this type of service or system as operated or offered by a library or educational institution."

NEW SECTION. **Section 5. Effective date.** [This act] is effective on passage and approval.

NEW SECTION. **Section 6. Codification instruction.** [Section 1] is intended to be codified as an integral part of Title 20, chapter 7, part 13, and the provisions of Title 20, chapter 7, part 13, apply to [section 1].

NEW SECTION. **Section 7. Applicability.** [This act] applies to contracts executed pursuant to [section 2] on or after [the effective date of this act].

- END -