SENATE BILL REPORT
ESSB 5316

As Passed Senate, March 4, 2015

Title: An act relating to privacy and security of personally identifiable student information.

Brief Description: Concerning privacy and security of personally identifiable student information.

Sponsors: Senate Committee on Early Learning & K-12 Education (originally sponsored by Senators Dammeier, Rolfes, Rivers, Hasegawa, Brown, Frockt, Dansel, Braun, Chase, Angel and Kohl-Welles).

Brief History:
Committee Activity: Early Learning & K-12 Education: 1/29/15, 2/12/15 [DPS, w/oRec].
Passed Senate: 3/04/15, 47-1.

SENATE COMMITTEE ON EARLY LEARNING & K-12 EDUCATION

Majority Report: That Substitute Senate Bill No. 5316 be substituted therefor, and the substitute bill do pass.
Signed by Senators Litzow, Chair; Dammeier, Vice Chair; McAuliffe, Ranking Member; Billig, Fain, Rivers and Rolfes.

Minority Report: That it be referred without recommendation.
Signed by Senator Mullet.

Staff: Ailey Kato (786-7434)

Background: Family Educational Rights and Privacy Act (FERPA). This federal law protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when the student reaches the age of 18 or attends a school beyond the high school level.

Under FERPA schools generally must have written consent from the parent or student, when the right has transferred, in order to release any personally identifiable information from a student's education record. However, there are exceptions to this consent requirement.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

A federal regulation defines personally identifiable information as including, but is not limited to, the following:

- the student's name;
- the name of the student's parent or other family members;
- the address of the student or student's family;
- a personal identifier, such as the student's social security number, student number, or biometric record;
- other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

A federal regulation defines biometric record, as used in the definition of personally identifiable information, as a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

FERPA does not apply to student data that has been aggregated and therefore no longer contains personally identifiable information.

Washington Law. Current law provides that the confidentiality of personally identifiable student data must be safeguarded consistent with the requirements of FERPA and applicable state laws. It also states that any agency or organization that is authorized by the Office of Superintendent of Public Instruction (OSPI) to access student-level data must adhere to all federal and state laws protecting student data and safeguarding the confidentiality and privacy of student records.

Current law provides that the board of directors of each school district must establish a procedure for granting parents' or guardians' requests for access to the education records of their child.

K–12 Data Governance Group. In 2009 the K–12 Data Governance group was established within OSPI to develop policies, protocols, and definitions for collecting data from school districts.

Special Education. Federal law requires each school district to provide special education for students who need it due to a disability. Under federal law an Individualized Education Program (IEP) or a section 504 plan guides the delivery of the special education supports and services designed to meet the child’s unique needs.

Summary of Engrossed Substitute Bill: Biometric Data. The following entities and people are prohibited from collecting, retaining, or using in any manner, student biometric information:

- the Superintendent of Public Instruction, or any employee or contractor of OSPI;
- an educational service district board of directors, employee, or contractor; and
- a school district board of directors, employee, or contractor.

However, biometric information may be collected, retained, or used if it is necessary to implement an IEP or section 504 plan.

Biometric information means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

Parent or Guardian Access to Personally Identifiable Data. OSPI must grant parents and legal guardians access to any student record that is a record of a child of the parent or a child in the care of the legal guardian, including records that contain personally identifiable data, unless the student is age 18 or older.

The board of directors of each school district must establish a procedure for granting parents' or guardians' requests for access to the education records of their child that provides the following:

- records must be provided electronically, if practicable;
- no fees are charged for the inspection of records; and
- if the records are provided in a non-electronic format, then the school district may impose a reasonable charge to cover the actual costs directly incident to the copying.

Protecting Personally Identifiable Data. All public agencies or organizations and private contractors or vendors that are authorized by OSPI, educational service districts, the board of directors of a school district, or any school in a district to access data must adhere to all federal and state laws protecting student data and safeguarding the confidentiality and privacy of student records. These public and private entities must ensure the following if they receive personally identifiable student-level data:

- All personally identifiable student data is used solely for the purpose for which the disclosure was intended;
- No personally identifiable student-level data is sold or used for secondary purposes such as marketing or targeted advertising;
- All personally identifiable student-level data, including backup copies, is destroyed when it is no longer required for the purposes for which it was disclosed, or upon agreement or contract termination, or project completion;
- A record is kept of any requests for access to the personally identifiable student-level data; and
- No personally identifiable student-level data is disclosed to any other individual or entity without the prior written consent of the parent, legal guardian, or student if the student is age 18 or older unless the entity is an educational agency or institution that abides by the foregoing data security requirements and FERPA.

These requirements do not apply to use or disclosure of personally identifiable student-level data by a private contractor or vendor to a service provider, provided the private contractor or vendor:

- prohibits the service provider from using any personally identifiable student-level data for any purpose other than providing the contracted service to, or on behalf of, the private contractor or vendor for the educational purposes for which such data was originally disclosed to the private contractor or vendor;
- prohibits the service provider from disclosing any personally identifiable student-level data provided by the private contractor or vendor to subsequent third parties unless the disclosure is otherwise permitted; and
- requires the service provider to comply with the foregoing requirements.

Personally identifiable student-level data means any information collected by OSPI, any state or local educational agency or institution, the board of directors of a school district, or any third-party service provider or contractor on behalf of the foregoing related to a particular identified or identifiable student in Washington, including, but not limited to the following:

- the student's name;
- the name of the student's parent or other family members;
- the address of the student or student's family;
- a personal identifier, such as the student's social security number, or student number;
- other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- 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 the student with reasonable certainty; or
- information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Personally identifiable student-level data does not include any anonymous and aggregated data that cannot be used to link specific information to a particular student.

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 personally identifiable data. Targeted advertising does not include advertising to a student at an online location based upon that student's current visit to that location or single search query without collection and retention of a student's online activities over time or across different web sites or applications.

Any public agency or organization that possesses personally identifiable student-level data must take special precautions to avoid accidental disclosure of the data, including encryption whenever feasible.

Private contractors or vendors must employ industry standard methods to ensure security of all personally identifiable student-level data that they receive, store, use, and transmit.

Nothing precludes the collection and distribution of aggregate data about students or student-level data without personally identifiable information.

Nothing precludes the release of directory information for the purpose of making available to parents and students school enhancement products and services as authorized by the educational service district, as long as any outside party receiving directory information for these purposes is prohibited from secondary use or sale of the information and is required to comply with all other provisions of this section. Directory information has the meaning assigned in FERPA and corresponding regulations. School enhancement products and services mean school-related products and services that are customarily offered under the direction or for the benefit of the public agency, organization, or school community, such as school photography, yearbooks, graduation products, and class rings.

Nothing prohibits the use of personally identifiable student-level data for adaptive learning, personalized learning, or customized education.

Nothing may be construed to impede the ability of students to download, export, or otherwise save or maintain their own student data or documents.

Data Security Plan. The K–12 Data Governance Group must develop a detailed data security plan and procedures to govern the use and maintenance of data systems, including ensuring the use of appropriate administrative, physical, and technical safeguards for electronic and physical personally identifiable student-level data at the state level.

The group must develop a model plan for school districts to use to safeguard personally identifiable student-level data at the school district level.

Appropriation: None.

Fiscal Note: Available.

Committee/Commission/Task Force Created: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony on Original Bill: PRO: In society, mass amounts of data are collected. Data is often used for good, but it can be misused. The government needs to be cautious about the data that it collects from students. Students do not have a choice to attend school, so the data that is collected from them needs to be protected. Currently our state relies heavily on federal law for student privacy. This bill covers a gap in state law. Biometric information can be used in many ways that we do not yet understand. It is improper to collect this data since it is not known how it will be used. De-identified information should be protected in the bill. The bill should state that data can only be used for educational purposes. The bill should strengthen encryption requirements. Online service providers that have contracts with schools want to make sure that this bill would not inhibit certain tasks such as getting addresses for transportation purposes and sending work home to students.

OTHER: There is no definition for personally identifiable information in Washington law. Adding a definition would strengthen the bill. Newspapers often run stories about student

achievement, and reporters want to make sure that information regarding achievement and recognition still could be shared with them. Certain bill language may unintentionally restrict use of data with contractors and researchers, which helps with school accountability. Operationalizing the detailed data security plan required by this bill will cost money. OSPI has a budget request for hiring a privacy records officer, which could help with implementing the plan.

Persons Testifying: PRO: Senator Dammeier, prime sponsor; Doug Klunder, American Civil Liberties Union of WA, Privacy Counsel; Carolyn Logue, K12, In.

OTHER: Dierk Meierbachtol, OSPI; Rowland Thompson, Allied Daily Newspapers.