SENATE BILL REPORT
SB 5316

As Reported by Senate Committee On:
Early Learning & K-12 Education, February 12, 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: 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].

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.

Summary of Bill (Recommended Substitute): 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.

Biometric information includes, but is not limited to, a fingerprint or hand scan, a retina or iris scan, a voice print, or a facial geometry scan of a student.

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.

Third Party Disclosure of Personally Identifiable Data. OSPI and the board of directors of school districts must not disclose personally identifiable student-level data to any other third party unless the disclosure is necessary to meet the following:

- a legitimate need for the data to support the particular student's education, or
- the needs of an educational study or educational purpose specifically authorized by a public agency.

However, nothing limits disclosure of information allowed under FERPA.

Personally identifiable student-level data means any information relating to a particular identified or identifiable individual including, but not limited to, any deidentified data that relates to a particular identified or identifiable individual, but not including any anonymous and aggregated data that cannot be used to link specific information to a particular student.

OSPI and school district boards of directors may release directory information for the purpose of making available to parents and students school enhancement products and services as authorized by OSPI and school district boards of directors, 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 requirements. 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.

Protecting Personally Identifiable Data. All public agencies or organizations and private contractors or vendors that are authorized by OSPI or the board of directors of a school 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 must be used solely for the purpose for which the disclosure was specifically intended;

- No personally identifiable student-level data may be used for marketing, commercial, or advertising purposes;
- All personally identifiable student-level data, including backup copies, must be destroyed when the data is no longer needed, or upon agreement or contract termination, or project completion;
- Parents and legal guardians must be granted 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;
- A record must be kept of any requests for access to the personally identifiable student-level data; and
- No personally identifiable student-level data may be disclosed to any other individual or entity without the prior written consent of the parent, legal guardian, or student if the student is over the age of 18 unless the entity is a designated education agency that abides by the data security requirements of this section.

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 of encryption, in transit and at rest, for all personally identifiable student-level data that they receive, store, use, and transmit.

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.

EFFECT OF CHANGES MADE BY EARLY LEARNING & K-12 EDUCATION COMMITTEE (Recommended Substitute): A definition for personally identifiable student-level data is added. Personally identifiable student-level data must not be disclosed to any other third party unless the disclosure is necessary to meet (1) a legitimate need for the data to support the particular student's education; or (2) the needs of an educational study or educational purpose specifically authorized by a public agency. However, nothing limits disclosure of information allowed under FERPA. A provision is added that allows personally identifiable student-level data to be disclosed without prior written consent if the entity is a designated education agency that abides by the data security requirements. OSPI and school districts may release directory information for the purpose of making available to parents and students school enhancement products and services as authorized by OSPI and the school districts, 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 requirements. 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. 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 of encryption, in transit and at rest, for all personally identifiable student-level data that they receive, store, use, and transmit.

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.