WISCONSIN LEGISLATIVE COUNCIL
STAFF MEMORANDUM

Memo No. 1

TO: MEMBERS OF THE STUDY COMMITTEE ON SCHOOL DATA

FROM: Katie Bender-Olson, Senior Staff Attorney, and Brian Larson, Staff Attorney

RE: Options for Further Study Committee Consideration

DATE: September 7, 2016

This Memo summarizes options for further consideration by the Study Committee on School Data. The options were raised by speakers and committee members at the July and August committee meetings. The Memo is intended to assist the committee by serving as a starting point for discussion. Committee members may have additional issues that they wish to present for consideration that are not described in this Memo.

Study committees generally present recommendations to the Joint Legislative Council in the form of proposed legislation. However, the committee may also make recommendations in an alternative manner, such as through a letter or report highlighting issues for further action or study by the Legislature.

STUDENT DATA PRIVACY OFFICER

Background

The Wisconsin Department of Public Instruction (DPI) currently employs a "Data Governance Coordinator" with responsibilities relating to technology security and privacy of student data. The position and responsibilities are assigned at the discretion of the State Superintendent, and are not specifically required by state law.

Speakers and committee members discussed legislation in other states establishing a "Chief Privacy Officer" or "Data Governance Officer" responsible for ensuring privacy and security of student data. These officers are typically assigned at least some statutory duties, but the extent and detail of the assigned duties varies among states. Some states assign only limited and general responsibilities, such as ensuring security of student data and developing best practices regarding student data. Other states assign specific, enumerated responsibilities, such

One East Main Street, Suite 401 • P.O. Box 2536 • Madison, WI 53701-2536
(608) 266-1304 • Fax: (608) 266-3830 • Email: leg.council@legis.wisconsin.gov
http://www.legis.wisconsin.gov/lc

as conducting privacy impact assessments on legislative proposals and operating a privacy incident response team to respond to data breaches.

The following are examples of responsibilities assigned to privacy officers in other states:

- Ensure compliance with privacy laws. Georgia and West Virginia require that the privacy officer ensure that the state department of education handles student data in full compliance with state and federal data privacy and security laws.

- Evaluate legislative proposals. West Virginia requires that the privacy officer evaluate any legislative or regulatory proposals involving use, collection, and disclosure of student data by the state department of education. Georgia requires the privacy officer to complete a privacy impact assessment on proposed legislation or administrative rules.

- Engage with stakeholders. Georgia and West Virginia require the privacy officer to engage with stakeholders and governmental officials regarding the quality, usefulness, openness, and privacy of student data.

- Report to the Legislature. Georgia requires the privacy officer to prepare and submit an annual report to the Legislature on activities of the state department of education that affect privacy, including complaints of privacy violations, internal controls, and other matters.

- Establish a privacy incident response program. Georgia and West Virginia require the privacy officer to establish and administer a response program to ensure that incidents involving student data held by the state department of education are properly reported, investigated, and mitigated.

- Develop a model security plan for school districts. Virginia requires the privacy officer to develop a model security plan including items such as: (a) guidelines for access to student data; (b) privacy compliance standards; (c) privacy and security audits; (d) procedures to follow in the event of a student data breach; and (e) data retention and disposition policies.

- Implement or develop a model process for complaints of privacy violations. West Virginia requires the privacy officer to establish and operate a process within the state department of education for receiving and responding to parent complaints of privacy violations and for providing redress. Georgia requires the privacy officer to create a model policy for school districts that establishes a process for parents or eligible students to file complaints about violations of student privacy or inability to access student records.

Speakers and committee members also raised the following as potential responsibilities of a student data privacy officer:

- Provide training, guidance, technical assistance, and outreach to school districts. Members discussed requiring a student data privacy officer to provide training and assistance regarding student data privacy protection and data security to school districts.
- Develop best practices. Members discussed requiring a student data privacy officer to develop recommendations for school districts regarding use, retention, and protection of student data.

Option 1: Require a Student Data Privacy Officer

The committee could consider requiring a designated officer within DPI who has responsibilities related to maintaining the security of student data, and could consider assigning the officer general or specific duties. Assigned responsibilities could include any or all responsibilities required in other states or raised during committee discussion.

Option 2: Assign Responsibilities Directly to DPI

The committee could consider assigning identified responsibilities to DPI, rather than a designated student data privacy officer. Any or all responsibilities required of the privacy officer in other states or raised during committee discussion may be generally assigned to the agency.

STATE DATA INVENTORY

Background

DPI provided a data inventory and Student Data Fact Sheet to the committee prior to the August 16, 2016 meeting. However, state law does not currently require DPI to develop or post a data inventory.

Speakers and committee members discussed legislation in other states requiring the state department of education to create and publish a "data inventory" listing the student data elements collected by that department. Some states also require the department to provide definitions of the student data elements and to regularly update the data inventory.

The following are examples of data inventory requirements in Georgia, Oklahoma, Idaho, and Tennessee:

- A list of all student data elements reported to the state department of education.
- A dictionary or index with definitions of data elements.
- A statement of the purpose or reason for collecting each data element.
- A list of data elements collected or maintained that have no current identified purpose.

- A notation regarding any new data element the state department of education proposes to begin collecting.
- Annual updates to the data inventory and index of data elements (Idaho).

Speakers and committee members also raised the following as possible data inventory requirements:

- A citation to the federal or state law requiring collecting of each data element.
- The source of each data element.

Option: Require a Data Inventory

The committee could consider requiring DPI to create and publish a data inventory of the student data elements it collects. In addition, the committee could incorporate any or all data inventory requirements mandated in other states or raised during committee discussion.

RESTRICTION ON COLLECTING NEW DATA ELEMENTS

Background

Committee members discussed prohibiting DPI from collecting additional student data elements unless certain conditions were met. Some states require their departments of education to fulfill notification requirements or requirements for a public review and comment period about a proposed new student data element.

The following are examples of conditions that must be met in other states before the state department of education may collect additional student data:

- Notify the Legislature of any proposed new data element. (Georgia, Oklahoma)
- Notify the Governor of any proposed new data element. (Georgia, Oklahoma)
- Require the department of education to publicly announce its intention to collect a new data element and hold a 60-day public review and comment period. (Georgia, West Virginia)
- Allow the department of education to begin collecting a new data element, but require it to stop collecting the element if the department does not receive legislative approval by the end of the next legislative session. (Oklahoma)
- Allow the department of education to begin collecting a new data element, but require it to stop collecting the element if the agency does not promulgate an administrative rule requiring such collection within one year. (Idaho)

Speakers and committee members also raised the following as possible conditions that could apply prior to collection of additional data elements by DPI:

- Review by the Joint Committee on Information Policy and Technology.

- Review by other legislative committees, such as the Assembly and Senate education committees.

Option: Prohibit DPI From Collecting Additional Student Data Elements Unless Certain Conditions Are Met

The committee could consider prohibiting DPI from collecting any new student data element, except as required by state or federal law, unless certain conditions are met. The conditions could include any or all requirements mandated by other states or raised during committee discussion.

One possible condition raised during committee discussion would require review by the Joint Committee on Information Policy and Technology or another legislative committee. This committee review could require: (a) an affirmative vote by the committee before DPI may collect a new data element; or (b) passive review whereby DPI is only prohibited from collecting the new element if the committee votes to object.

STATEMENT OF LEGISLATIVE INTENT

Background

Several states have included a statement of legislative intent in measures enacted to protect student data security and privacy. For example, the Idaho Legislature included a lengthy statement acknowledging the educational value of student data while expressing an intent to protect student privacy and data security. Idaho law labels student data a "vital resource" that is "important for educational purposes," but states that "it is also critically important to ensure that student information is protected, safeguarded and kept private and used only by appropriate educational authorities and then, only to serve the best interests of the student."

The policy of the Wisconsin Legislative Reference Bureau (LRB), the state's drafting agency, has been to avoid statutory language expressing legislative intent, purpose, or findings. This policy is rooted in concerns that a statement of intent could create conflicts in the statutes or have other unforeseen effects as laws are changed over time. However, LRB policy is not binding upon the Legislature, and state law contains some provisions of legislative intent, such as in the case of the Open Records Law.

Option: Statement of Intent

The committee could consider including a statement of legislative intent in state law regarding student data privacy and security. The statement could focus specifically on data privacy and security. Alternatively, it could express a balancing of student data privacy and security against other interests, such as the educational value of the data.

REGULATION OF THIRD-PARTY VENDORS

Background

Speakers and committee members discussed legislation in other states regulating the collection of student data by entities that operate educational apps and online education services or websites. For example, under California law, such vendors are prohibited from selling a student's information, using a student's information to amass a profile about the student, or knowingly engaging in targeted advertising to students or their parents or legal guardians. A similar restriction has been enacted in Georgia.

In those states, purposes for which collection and use of student data are not authorized include the following:

- Selling collected data to any other person or entity.
- Disclosing collected data to any other person or entity, except as otherwise provided by law.
- Amassing a profile about a K–12 student.
- Knowingly engaging in targeted advertising to students or their parents or legal guardians.
- Any other use, unless the entity has implemented specified security procedures and practices to protect the information from unauthorized access, use, or disclosure, and to ensure that student data collected by the entity will be deleted at the request of the student or his or her family.

Option: Prohibit Vendors From Unauthorized Use

The committee could consider prohibiting entities that operate educational apps and online education services or websites from collecting and using student data for unauthorized purposes, such as those identified above.

RETENTION AND DISPOSITION OF STUDENT DATA

Background

DPI retains student data in its longitudinal database indefinitely, according to testimony received by the committee. On its own initiative, DPI could shorten the length of time certain data is retained, subject to the approval of the Public Records Board. With a statutory change, the Legislature could also impose more specific requirements on DPI, such as a requirement to retain certain data for at least a specified length of time, or to dispose of certain data after a specified length of time.

Option 1: Retention of Data

The committee could consider requiring DPI to retain student data in its longitudinal database indefinitely, as under current practice, or for at least a specified length of time, such as 15 years. This requirement could apply to all data collected by the department, or to certain data elements specified by the committee. If a length of time is specified in statute, it would remain possible for DPI to retain data for a longer period, on its own initiative.

Option 2: Disposition of Data

The committee could consider requiring DPI to dispose of student data in its longitudinal database after a specified length of time, which would prohibit the current practice of indefinite retention. This requirement could apply to all data collected by the department, or to certain data elements specified by the committee. If a length of time is specified, it would remain possible for DPI to dispose of data within a shorter period, on its own initiative, subject to Public Records Board approval.

Option 3: De-identified Copies of Disposed Records

In connection with Option 2, the committee could consider requiring data elements that must be disposed of to be retained in de-identified form, rather than completely destroyed. This would allow educational researchers to continue to have access to the aggregate data following disposition of identified records.

OWNERSHIP AND ACCESS TO STUDENT DATA

Background

Speakers and committee members discussed practices in other states relating to ownership of and access to student data. Federal law gives parents and eligible students the opportunity to inspect and review many student records. Some states have built upon this requirement by adding procedures to enable students and families to have greater access to and control over student data. For example, Georgia and Utah have taken steps to enable students and families to compile copies of records that they deem most important, which facilitates the sharing of that data. Georgia gives families the right to receive electronic copies of student records upon request. Utah has adopted the "data backpack" concept into its law, which allows students and families to identify certain records that the Utah State Office of Education will maintain, in electronic form, on behalf of the student. These laws facilitate access to a range of records beyond traditional assessment data, including teacher's notes and individualized educational plan summaries, if they are maintained in an electronic form.

Option 1: Electronic Copies of Student Records

The committee could consider requiring DPI to give students and families electronic copies of certain records upon request. The committee could apply the requirement to all records maintained in electronic form, or to certain records specified by the committee.

Option 2: Data Backpack

The committee could consider requiring DPI to make available a "data backpack" option for students and families by allowing them to identify certain records that DPI would be required to maintain, in electronic form, on behalf of the student. The committee could apply the requirement to all records maintained in electronic form, or to certain records specified by the committee.

Option 3: Ownership and Access in Connection with Disposition and Retention

Procedures to enable students and families to have greater access to and control over student data, such as those in Options 1 and 2, could be coupled with measures regarding retention or disposition of data. For example, if legislation required DPI to make a data backpack available to allow students and families to "select" certain data to be saved, the legislation could require data elements that are **not** selected to be disposed of after a specified length of time.

Option 4: District Support

The committee could consider measures to assist school districts that choose to implement policies at a local level. Legislation could require DPI to develop a model policy regarding ownership of and access to student data, and to provide training and assistance to local school districts regarding such policies. Assistance to school districts could be considered in lieu of, or in addition to, Options 1, 2, and 3.

KBO:BL:ksm