Student Data Privacy Council Report

to the

Governor and General Assembly,

as required by the

The Student Data Privacy Council Act
(HB 245, RS 2019)

Presented by the

Maryland State Department of Education

December 31, 2020

Larry Hogan
Governor

Karen B. Salmon, Ph.D.
State Superintendent of Schools

MARYLAND STATE DEPARTMENT OF EDUCATION
200 West Baltimore Street
Baltimore, Maryland 21201
410-767-0100
MarylandPublicSchools.org

Karen B. Salmon, Ph.D.
Superintendent of Schools

Clarence C. Crawford
President, Maryland State Board of Education

Larry Hogan
Governor

Carol A. Williamson, Ed.D.
Deputy State Superintendent
Office of Teaching and Learning

Contents

Background

During the 2014 and 2015 legislative sessions, state lawmakers across the country began grappling with a new issue: student data privacy. Amid the explosion of legislative activity around student data privacy, the Maryland legislature passed the Student Data Privacy Act of 2015 (SDPA) in a vote of 128-11. Addressing some pieces of the student data privacy issue, the SDPA aims to protect public students' privacy by governing how private sector technology companies handle students' information. In particular, the SDPA prohibits technology vendors (operators) who are operating under a contract or agreement with a public school or local public school system from collecting and analyzing individual student's data in order to develop profiles of specific students for marketing, advertising, or sales purposes. The SDPA also mandates that the operators take proactive steps to protect students' data from unauthorized access, safeguard students' data against breaches, and return students' data to the schools once the contract or agreement expires.

During the 2019 legislative session, Maryland lawmakers passed the Student Data Privacy Council bill (HB 0245). The bill established the Student Data Privacy Council (the Council) to study how well the Student Data Privacy Act of 2015 is protecting the privacy of students, whether it's keeping pace with technology, and is generally operating as intended. To complete its tasks the bill identified student privacy experts, technology officers, parents, and administrators as members of the Council. By December 31, 2020, the Council must report its findings and recommendations to the Governor and General Assembly, including whether the Council should be made permanent and if so, what its function should be. The bill took effect June 1, 2019, and terminates May 31, 2021.

Charge

The enacting legislation outlined the charge of the Council, requiring the Council to study and make recommendations, and report those findings and recommendations. Under the enacting legislation, the Council was required to[1]:

1. Study the development and implementation of the Student Data Privacy Act of 2015 to evaluate the impact of the Act on:
    a. The protection of covered information from unauthorized access, destruction, use, modification, or disclosure;
    b. The implementation and maintenance of reasonable security procedures and practices to protect covered information under the Act; and
    c. The implementation and maintenance of reasonable privacy controls to protect covered information under the Act;
2. Review and analyze similar laws and best practices in other states;
3. Review and analyze developments in technologies as they may relate to student data privacy; and

[1] Maryland HB0245 (CH0398). Retrieved from http://mgaleg.maryland.gov/webmga/frmMain.aspx?id=hb0245&stab=01&pid=billpage&tab=subject3&ys=2019RS

4. Make recommendations regarding:
    a. Statutory and regulatory changes to the Student Data Privacy Act (SDPA) based on the findings of the Council; and
    b. Repeal of the termination date set by the Act that established the Council, to allow the Council to continue its evaluation of student data privacy in the State on a permanent basis.

Establishment of the Council

In June 2019, the State Superintendent of Education, designated Dr. Carol Williamson, Deputy Superintendent for Teaching and Learning, as chair of the Council. Four individuals from MSDE provided staff support to the Council.

Although the enacting legislation required membership from a variety of organizations, it did not specify the representatives. The MSDE worked with the leadership of the representative organizations and requested they nominate a person to represent them on the Council. The MSDE considered the size and location of organizations and the demographics of membership to ensure a diverse perspective and to inform the work of the Council. In August 2019, the Chair distributed letters to each of the identified member representatives inviting their participation on the Council, with the first meeting occurring in fall 2019. Members were asked to agree to attend all of the meetings or to have one designated person stand in for them whenever they were not able to attend. This helped ensure the discussions could move forward more efficiently and objectives could be accomplished more quickly since a continual review of background information and decisions from previous meetings was not necessary.

The enacting legislation required the Council to include the following members:

1) One member of the Senate of Maryland, appointed by the President of the Senate;
2) One member of the House of Delegates, appointed by the Speaker of the House;
3) The State Superintendent of Schools, or the Superintendent's designee;
4) The Secretary of Information Technology, or the Secretary's designee;
5) The Executive Director of the Public School Superintendents' Association of Maryland, or the Executive Director's designee;
6) The Executive Director of the Maryland Association of Boards of Education, or the Executive Director's designee;
7) The President of the Maryland State Education Association, or the President's designee;
8) The President of the Maryland PTA, or the President's designee; and
9) The following members appointed by the Chair of the Council:
    a) One School Data Privacy Officer, or the Officer's designee;
    b) One School Information Technology Officer, or the Officer's designee;
    c) One representative of a company, trade association, or group who has professional experience in the area of student data privacy or online educational technology services;
    d) One member of the academic community who studies K–12 student data privacy;

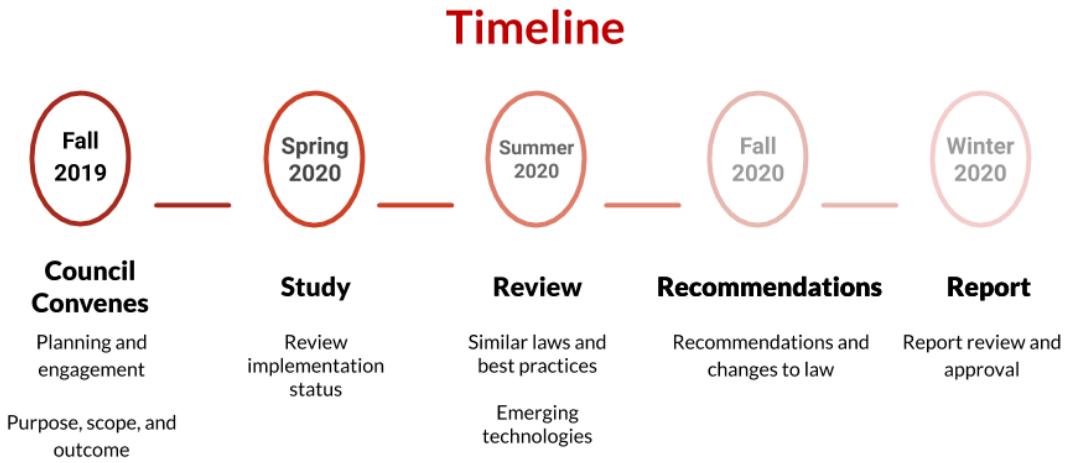
e) One advocate for student data privacy who does not have a professional relationship with a provider of online educational technology services;
f) One attorney who is knowledgeable in the laws and regulations that pertain to local school systems;
g) One school–based administrator from a public school in the State; and
h) One teacher from a public school in the State.

Detailed minutes of each meeting were taken and provided to members for review prior to each meeting. Minutes of the preceding meeting were approved at the next meeting and were then posted on the website, as all meetings were open to the public.

Meeting Format and Structure

The Council held a total of 14 meetings during the period of October 2019 to December 2020. Meetings were held at various locations throughout central Maryland, and beginning in March 2020, the meetings were held virtually. The Council systematically worked through the charge set in the legislation. Each meeting consisted of agenda topics to guide the work and meeting minutes provided to document the work and further the Council's understanding.

All meetings of the Council were open to the general public. Council Meeting Dates and Locations with the meeting agenda were posted in advance of each meeting. Meeting minutes were posted after approval of the Council. Specific norms and practices on the Council's roles and responsibilities, composition, meetings, and more were discussed and then approved by the Council in December 2019.



Findings of the Council

The Council concluded that the Student Data Privacy Act (SDPA) as a whole was sufficiently implemented though there are areas that need additional clarification, description, and adjustment.

While the SDPA places restrictions on "operators", the Council found that the burden for implementation of the SDPA was on local school systems (LSS). Further review of the local school system implementation demonstrated uneven operations in accordance with each local school system's interpretation of the SDPA. To address these areas the Council's recommendations focus on expanding clarity in the law, developing compliance mechanisms, and increasing transparency.

The enacting legislation outlined the charge of the Council and required the Council to study the development and implementation of the SDPA, to review and analyze similar laws and best practices of other states, and to review and analyze emerging technologies. For each of the requirements, the Council developed a set of "Guiding Questions" to guide the work. At each meeting, the Council received supporting information relevant to each guiding question, which included presentations by experts, opportunities to engage in facilitated discussions, and pertinent material to develop findings of the Council and to turn the guiding questions into recommendations.

This section of the report includes each of the requirements in the enacting legislation, the Guiding Questions, Council Findings, and supporting information in the form of meeting agendas and minutes.

Study the Development and Implementation of the Student Data Privacy Act of 2015

The Council interpreted "development and implementation" into three guiding questions around the national landscape, local school systems, and operators.

Guiding Questions for the Study of the Development and Implementation of the Student Data Privacy Act:

1. What does the national and Maryland's privacy landscape look like?
2. How have Maryland's local school systems implemented the Maryland Student Data Privacy Act?
3. How have Operators implemented the Maryland Student Data Privacy Act?

Findings in response to Guiding Question 1: *What does the national and Maryland's privacy landscape look like?*

Maryland – National Privacy Landscape

The Council found that student data privacy is a topic of interest across states based on the number of privacy laws that have passed in states over the last decade. Since 2013, over 130 new state student privacy laws have been passed, and over one thousand bills were introduced on the topic in all 50 states[2]. Among other things, the interest is fueled by an increase in the use of education technology, especially with remote learning, and the need to ensure the privacy of student data.

[2] Student Privacy Compass, State Student Privacy Laws

State student privacy laws tend to model the federal education privacy law, the Family Educational Rights and Privacy Act (FERPA), by directly regulating education agencies, or California's education privacy law, the Student Online Personal Information Protection Act (SOPIPA), by regulating both education agencies and vendors. Laws that follow the FERPA model typically require that schools establish control over education records, create a student-facing data portability requirement, prohibit the use of student data for commercial purposes or non-educational purposes, outline parental and student rights, require that schools ensure that vendors employ sufficient security and privacy practices, describe methods for notifying parents and students of a data breach, and ensure there is a set data retention period when contracting with third-parties. In contrast, over 20 enacted state student privacy laws follow the SOPIPA model. Generally, these laws prohibit vendors from using targeted advertising, creating profiles of students outside of an educational purpose, selling student information, and place limits on how vendors can appropriately disclose student information. These laws also require vendors to employ security and privacy best practices and ensure student information is deleted upon request from an education agency. Maryland's Student Data Privacy Act is modeled after SOPIPA.

Student data privacy concerns have increased during the COVID-19 pandemic as systems switch to remote, hybrid, or heavily monitored in-person learning environments. With online and hybrid learning environments, data gathered by LearnPlatform indicated that, on average per school district nationally, "1,327 ed-tech tools—were accessed on average each month after the coronavirus-related closures. That's a nearly 90 percent increase over the previous monthly average for the 2018-2019 academic year, when just 703, were accessed." As reliance on online tools increases, so does the need for adequate teacher training and understanding of student data privacy. As schools make efforts to facilitate in-person and hybrid learning environments, concerns about student data privacy should not hinder aggregate reporting of COVID-19 diagnoses to the school community, and should further efforts to ensure that individual student health information is collected, stored, and used in a privacy-protective manner.

The Importance of Student Data

The Council found that student data are valuable to parents, teachers, and the public, but that transparency and privacy are often at odds. While there are valid concerns about protecting the privacy of student data, those concerns should not curtail efforts to make meaning of aggregate or de-identified student data. For example, schools may want to publish transparent disciplinary reports, noting student suspensions by race to understand whether all students are being served equitably. In smaller school districts, those numbers may reveal which particular students received certain sanctions. In those circumstances, the school systems may need to suppress some of the student data in order to comply with education privacy laws, thus rendering the result less transparent but protecting student privacy.

The Data Quality Campaign (DQC) provided information obtained from parent and teacher surveys on the use of student data, to the Council. The Data Quality Campaign emphasized the importance of transparency in ensuring data are used in service to students.

Maryland Student Data Governance Act (HB0568, RS 2018)

The Council heard from representatives on the Council and the MSDE on the ongoing work by the Student Data Governance Workgroup to identify best practices in governance, transparency, and professional development. The Council concluded that local school systems policy development and implementation were under the purview of the Student Data Governance Act of 2018. The Workgroup was established by the MSDE in partnership with the Maryland Department of Information Technology (DoIT) in response to the Maryland Student Data Governance Act of 2018. Under the Act, LSSs are required to manage and maintain a data governance program, develop, and implement an incident response plan, a data breach plan, and researcher access procedures. LSSs are also required to provide annual notification on items such as types of student data and personally identifiable information (PII).

The MSDE submitted two reports to the Maryland General Assembly that included status updates on multiple areas and recommended statutory changes. The Student Data Governance Workgroup members were especially critical in the development of the recommendations submitted in the second report. The Student Data Governance Workgroup continues to meet periodically throughout the year. The Workgroup provides a space for LSS collaboration, MSDE technical assistance, a way to collectively identify areas of need within the state, and to identify areas of success.

The charge of the Council was specific to studying the development and implementation of the Student Data Privacy Act of 2015, to review and analyze similar laws and best practices of other states, and to review and analyze emerging technologies. The Council was presented information on the work from the Workgroup established for the Maryland Student Data Governance Act of 2018, however this report is focused on the charge of the Council as it pertains to the SDPA.

Guiding Question 1 Supporting Information:

Meeting Agenda	Agenda Item(s) and Presenter	Meeting Minutes
October 10, 2019	● Maryland – National Privacy Landscape, Presented by Sean Cottrell, SLDS State Support Team, U.S. Department of Education	Minutes
January 9, 2020	● Four Policy Priorities to Make Data Work for Students, Abigail Cohen, Data Quality Campaign ● Student Data Governance Workgroup Report, Chandra Haislet, Director, Accountability and Data Systems, MSDE	Minutes
June 11, 2020	● MSDE Student Data Governance Workgroup Report, Chandra Haislet	Minutes

Findings in Response to Guiding Question 2: *How have Maryland's local school systems implemented the Maryland Student Data Privacy Act?*

Procurement Processes to Support Student Privacy

The Council concluded that local school systems are often responsible for ensuring contracts with operators subject to the SDPA comply with the law, in the absence of other compliance or monitoring.

The Council explored the procurement processes at all levels of the state in studying the implementation of the SDPA. MSDE's Principal Counsel provided information on state procurement laws to the Council.

The Council found that larger local school systems have been more successful in implementing procurement procedures and checklists to ensure privacy of student data with contracted operators. Even the larger local school systems noted that they do not always have the leverage needed to compel operators to agree to and comply with State laws and local procedures. Local school systems noted instances in which contracts were not completed because operators would not agree or negotiate on conditions. Presenters and Council members representing local school systems all indicated issues with click-through agreements and software license agreements. This highlighted the burden placed on school systems to ensure operator compliance in the absence of enforcement mechanisms in the law.

The Maryland Education Enterprise Consortium (MEEC) and the Eastern Shore of Maryland Educational Consortium (ESMEC) presented ways local school systems may leverage resources to ensure the protection of student data. While MEEC offers many benefits to both vendors and MEEC members, MEEC does not offer professional development or training regarding contracts and data privacy.

Local School System Implementation

Transparency:

The Council found that nearly all local school systems had publicly available information on privacy and security. At the request of the Council, Council staff explored the local school systems' websites for material regarding privacy and security resources. Council staff reported that almost all local school systems had a public list of digital tools they deemed acceptable and such information as a description of the tool, student information shared, and subject areas covered. Few local school systems included on their website a process for suggesting, vetting, and approving digital tools or contract language between local school systems and operators. A presentation by Mr. Thomas Chapman, Assistant to Associate Superintendent in the Office of Technology and Innovation at Montgomery County Public Schools, described that system's process for vetting online digital tools, including establishing guidelines for selecting a digital tool and an online vetting form to request a review of new digital tools.

Challenges presented to the Council:

Currently each local school system must determine if an operator they seek to contract with is compliant or non-compliant, even if the operator contracts with other school systems in the state. Additionally, there is limited information on operators who have contracts with other local school systems. This adds additional burden to the local school systems. Local school systems noted the need for additional information and opportunities to leverage collective resources across the state. Examples of information that could inform local schools system decisions:

- Why a local school system has chosen not to contract with a particular operator;
- When an operator is not willing to negotiate; and
- Parent complaint (click-agreements).

While the Council agreed that some pooling of resources and information was valuable, it was outside the scope of the SDPA.

Impact of the Student Data Privacy Act:
The Council found that most local school systems had changed practices or operations in response to the Maryland SDPA. In March 2020, the Council requested local school system representatives complete a survey containing questions on SDPA implementation. All school systems responded and the Council discussed final results at its May 2020 meeting. Council members requested that the results of the local school system survey be disaggregated by system size to provide more context. Overall, 18 of 24 (75%) local school systems reported familiarity with Maryland's student privacy laws and the SDPA, with small and medium sized local school systems reporting less familiarity. Most (96%) LSSs reported that they had changed practices or operations in response to the SDPA but responses varied by system size. Large and medium sized LSSs tended to have formed groups for review of existing practices or operations. Small and medium sized LSSs were more likely to have finalized, upgraded, or added to their practices or operations.

The survey also found that large sized LSSs reported implementing processes for vetting online services for data privacy and security in 2017 or earlier as compared to small and medium sized systems. Additionally, large LSSs reported using a wider range of methods to educate LSS staff on vetting processes. Council members acknowledged this could be due to having processes in place for a longer period of time and access to more resources.

Guiding Question 2 Supporting Information:

Meeting Agenda	Agenda Item(s) and Presenter	Meeting Minutes
December 12, 2019	● Review of Local School System Information - Molly Abend, Data Management Coordinator, MSDE/MLDSC ● Proposed Local School System Survey - Laia Tiderman, Program Manager, MSDE ● Montgomery County Public Schools Implementation Experience - Thomas Chapman, Assistant to Associate Superintendent, Office of Technology and Innovation	Minutes
January 9, 2020	● Review of Proposed LSS Survey, Laia Tiderman, Program Manager, MSDE	Minutes
February 13, 2020	● Proposed LSS Survey - Council Staff ● Procurement Overview: Maryland - Law Elliott L. Schoen, Principal Counsel, MSDE ● Procurement Overview: Consortiums - Tamara Petronka, Executive Director, Maryland Educational Enterprise Consortium (MEEC) and Dr. Jeffrey Lawson, Superintendent Cecil County Public Schools, Eastern Shore of Maryland Educational Consortium (ESMEC)	Minutes
March 12, 2020	● Procurement Overview: Anne Arundel County Public Schools	Minutes
April 9, 2020	● Preliminary LSS Survey Results - Laia Tiderman	Minutes

Meeting Agenda	Agenda Item(s) and Presenter	Meeting Minutes
May 14, 2020	● LSS Survey Results - Laia Tiderman	Minutes
June 11, 2020	● LSS Survey Results - Laia Tiderman and Molly Abend	Minutes

Findings in response to Guiding Question 3: *How have Operators implemented the Maryland Student Data Privacy Act?*

Operator Implementation

The Council concluded that, while operators may generally adhere to student data privacy legal requirements, the SDPA contains a lack of accountability and enforcement for operators that is present in the laws of some other states. Utah's Student Privacy and Data Protection Act, places restrictions on future contracts or types of payments that may be required due to misuse of student data. Under Louisiana's Student Privacy Law unlawful disclosure of PII is punishable by a fine of no more than $10,000 or imprisonment for not more than 3 years, or both. New York's Education Law 2-D, includes per person (student or staff) civil penalties for third-party contractor breaches or unauthorized release of personally identifiable information under the state's general business law. Maryland's SDPA includes no similar penalties for operators.

Council members heard presentations on operators' individual experiences with the SDPA and student data privacy overall. In recent years operators reported updating data privacy policies, creating positions specific to data privacy, and engaging in varying levels of internal and external training. These changes appear to be influenced by the changing data privacy landscape and not in direct response to Maryland law. Though the College Board noted that because of Maryland's SDPA, Maryland's local school systems were "very proactive in reaching out to us [College Board] on issues that helped us refine our privacy practices."

Defining Operators

The Council found that the definition of the term "Operator" in the SDPA needs further clarification. Mr. Baron Rodriguez (the Council's advocate for student data privacy who does not have a professional relationship with a provider of online educational technology services) presented information on other states' operator clauses and potential issues. A main consideration informing the recommendation to clarify the definition was that many states currently define Operator to exclude companies that did not start as education technology companies unless they have created a specific product developed and marketed for schools, even though many schools contract with and provide those companies with student data. Although the school is bound by both federal and state student privacy laws in these cases, the company is often not, putting the student data held by the company at risk of being commercialized or otherwise inappropriately treated.

Guiding Question 3 Supporting Information:

Meeting Agenda	Agenda Item(s) and Presenter	Meeting Minutes
March 12, 2020	• Operator's Perspective - Michele McNeil, Vice President, Policy, Global Policy & External Relations, The College Board • Operator Agreements - Baron Rodriguez, Noble Privacy Solutions LLC	Minutes
June 11, 2020	• Generate Questions for Invited Operators - Council Members	Minutes
July 9, 2020	• Operator Panel Presentations - Discovery Education, Stephanie Milikh, General Counsel; BrainPop Shiri Levi-Kluska, General Counsel, Key Accounts (Northeast/MidAtlantic); Tech4Learning Scott Loomis, Mid-Atlantic Regional Manager	Minutes
August 13, 2020	• Council Discussion on Invited Operator Presentations - Council Members	Minutes

Review and Analysis of Similar Laws and Best Practices in Other States

The Council identified three guiding questions to support the requirement to review and analyze similar laws and best practices in other states.

Guiding Questions for review and analysis of similar laws and best practices in other states

4. How do other state's student data privacy laws compare to the SDPA?
5. What are student data privacy best practices from other states?
6. Is the SDPA current and comprehensive?

Findings in response to Guiding Question 4 Findings: *How do other states' student data privacy laws compare to the Maryland Student Data Privacy Act?*

Other State's Student Data Privacy Laws

The Council reviewed state laws from California, Utah, New York, and Louisiana.

California's Student Online Personal Information Protection Act (SOPIPA) (Cal. Bus. & Prof. Code §22584) was the first law to address student data privacy. Over 20 states, including Maryland, used SOPIPA as the basis for their privacy legislation framework. Other states that modeled student privacy laws after California's SOPIPA include Arizona, Connecticut, Delaware, Maine, Michigan, and Nebraska[3]. The law has requirements around operator use of student data and specifically prohibits targeted advertising.

Utah's Student Privacy and Data Protection Act (Utah Code Ann. §53E-9-301(14) (c) focuses mainly on data privacy policies and less so with security, but notably included a funding component to implement the requirements of the law. The law provides Utah's State Education Agency with dedicated student privacy staff that are equipped to provide technical assistance to local education agencies and

[3] Future of Privacy Forum, FPF Guide to Protecting Student Data Under SOPIPA, November 2016

continuously develop resources such as model contracts. One specific role created is that of the Student Data Privacy auditor, who periodically reviews district data governance plans to ensure alignment with the law.

The Council found New York's Education Law 2-D (N.Y. Educ. Law §2-D) inclusion of a state-level privacy officer and parent bill of rights would have some applicability to Maryland. The law also allows parents to file a complaint in the event of a data breach. The law requires specific security standards; vendors must implement HIPAA level encryption. In January 2020, the State Education Agency finalized regulations that impose strict contracting requirements, including requiring both vendors and education agencies to employ the National Institutes Standards and Technology (NIST) Cybersecurity Framework. Along with the strict, unique contracting requirements, the law places a large burden on schools to ensure that vendors are in compliance with the law and regulations. Because of the restrictive requirements, there is a risk that ensuring compliance will overburden schools and lock vendors out of the region, limiting educational opportunities for students.

Louisiana Student Privacy Law (La. Rev. Stat. Ann. §17:3914) is a dense and restrictive law, with complex language that makes it difficult to identify the responsible parties. Louisiana's law also includes strict penalties (criminal and financial) for unlawful disclosure of personally identifiable information (including penalties for mistakes). School districts in Louisiana are prohibited from sharing personally identifiable student information without parental consent, in any circumstance. The language of the law prevents schools from being able to recommend students for scholarships, share sports statistics, or more, without requiring parental consent for every instance. The Louisiana State Department of Education reached out to the U.S. Department of Education, Student Privacy Policy Office for additional guidance on enrollment data and disclosure avoidance. More recently, Louisiana's student data privacy law prevented Louisiana state agencies from knowing which families were eligible for Pandemic Electronic Benefits Transfer meal assistance for several months during the COVID-19 pandemic[4].

Findings in response to Guiding Question 5 Findings: *What are student data privacy best practices from other states?*

Best Practices from Other State Data Privacy Laws

After a review of the student data privacy laws in other states the Council identified the following best practices:

1. *Accountability*. The law should clearly identify violations. The law should name the agency or process through which violations may be reported, the options for enforcing compliance, and provide for penalties for non-compliance. Members recommended that Maryland law should have some form of a complaint process for parents.
2. *Intent*. The law should be proactive rather than reactionary and should consider unintended consequences and undue burden to local school systems (i.e. Louisiana).

[4] Paige Kowalski, Lesson from the State of Louisiana — If Your Student Privacy Laws Are Making Kids Go Hungry, There's a Problem, December 1, 2020

3. *Clarity.* Laws should include clear definitions and expectations for all identified parties.
4. *Sustainability*. Student data privacy laws require on-going attention from all stakeholders, not just the parties identified in legislation. Laws should engage stakeholders at all levels to support implementation, monitor the current status, and conduct annual reviews. Ongoing review of the law by the identified stakeholders and legislators is important to ensuring the law remains applicable and aligned to the intended purpose (i.e. Utah).
5. *Roles and responsibilities.* Laws should identify specific positions, such as a chief privacy officer, and the responsibilities and authority assigned to those roles.
6. *Resources and Funding*. Laws with dedicated funding can assist in training, oversight, and implementation. The most comprehensive laws included funding that was centralized at the State level with resources deployed to each local school system. State resources were then used to provide ongoing training or develop model policies. The centralized system ensured equity across the state and reduced burden to local school systems.

Guiding Questions 4 and 5 Supporting Information:

Meeting Agenda	Agenda Item(s) and Presenter	Meeting Minutes
February 13, 2020	● Overview of Similar Laws from Other States - Amelia Vance, Senior Counsel (Child Privacy) and Director of Education Privacy, Future of Privacy Forum	Minutes
March 12, 2020	● Small group study of Similar Laws - Council Members	Minutes
April 9, 2020	● Similar Laws Review - Council Members	Minutes

Response to Guiding Question 6 Findings: ***Is the Maryland Student Data Privacy Act current and comprehensive?***

Is the scope current and comprehensive?

The SDPA requires operators to protect student data from unauthorized access, implement and maintain security procedures and practices, and delete student specified information under specified circumstances. The SDPA prohibits operators for knowingly engaging in specified activities particularly related to target advertising. The SDPA defines operators as a person who is operating in accordance with a contract or an agreement with a public school or local school system in the state to provide an internet web site, an online service, an online application, or a mobile application that:

- is used primarily for a PreK–12 school purpose;
- is issued at the direction of a public school, a teacher, or any other employee of a public school, local school system, or the department; and
- Was designed and marketed primarily for a PreK–12 school purpose.[5]

[5] The Council recommendations include changes to the definition of "Operator." See the Appendix for proposed definitions.

The Council concluded that while the narrow scope of the SDPA may be appropriate, there is little oversight of the operators in legislation. Review of other state laws and best practices highlighted the lack of accountability in the SDPA. The Council noted the lack of notification of operator violations or inappropriate behaviors and practices. The members concluded that ensuring accountability of operators was a high priority and a recommendation of the Council. The Council discussed concerns in regards to the gaps in training and professional development to both the local school system and vendor staff.

The Council grappled with the separation of the overarching responsibilities of the local school systems to ensure the protection of student data from the specific requirements of SDPA. The Council concluded that the SDPA addresses how operators can and cannot use student data; the Student Data Governance Workgroup addresses the requirements for local school systems to protect student data.

Definitions

The Council determined that clear definitions are needed to ensure the SDPA is comprehensive. The Council concluded that the definitions in the SDPA were not as clear as needed to ensure the appropriate parties adhere to the law. The Council shared concerns that the definition of who constitutes an operator are limited, the SDPA only governs operators based on contracted services with local school systems, only covers targeted advertising, and is solely focused on how operators can and cannot use student data.

The Council agreed to have a small workgroup, consisting of three Council members and one MSDE staff person, work on reviewing and revising the definitions. The workgroup met several times from January to April. The workgroup made changes to four of the five definitions in the original SDPA based on Council discussions and workgroup members' expertise and knowledge of other state laws. At the August 2020 meeting, the Council approved the definitions to be included in its recommendations. The complete definitions with the recommended changes are included in the Appendix.

Guiding Question 6 Supporting Information:

Meeting Agenda	Agenda Item(s) and Presenter	Meeting Minutes
October 10, 2019	● Overview of Council purpose and enacting legislation - Council Members	Minutes
November 12, 2019	● Student Data Privacy Act of 2015: ○ Independent study of the Act - Council Members ○ Discussion of intent of original legislation - Theodore Hartman, Howard County	Minutes
January 9, 2020	● Establishing Definitions - Laia Tiderman	Minutes
April 9, 2020	● Relevant Definitions - Molly Abend	Minutes
May 14, 2020	● Relevant Definitions - Molly Abend ● Identified Issues from Legislative History - Laia Tiderman	Minutes

Meeting Agenda	Agenda Item(s) and Presenter	Meeting Minutes
	● Discussion of Gaps in the Student Data Privacy Act of 2015 - Council Members	
June 11, 2020	● Continued Discussion of Issues in the Student Data Privacy Act of 2015 - Council Members	Minutes
August 13, 2020	● Review of Issues in the Student Data Privacy Act of 2015 - Carol Williamson	Minutes

Review and Analysis of Emerging Technologies

The Council identified two guiding questions to support the requirement to review and analyze emerging technologies.

Guiding Questions for review and analysis of emerging technologies:

7. What is the impact of emerging technology on the Maryland Student Data Privacy Act?
8. How do current and emerging technologies change the requirements of the Maryland Student Data Privacy Act?

Findings in response to Guiding Questions 7 and 8 Findings: What is the impact of emerging technology and do current and emerging technologies change the requirements of the Maryland Student Data Privacy Act?

Keeping pace with emerging technology

The Council concluded that while emerging technology vendors might need more understanding of the complexities of student data privacy, Maryland's Student Data Privacy Act is applicable to current and future emerging technology operators.

The Council had recurring questions about whether technology has outpaced the SDPA since its passage in 2015. To address these concerns, MSDE's Director of Instructional Technology reviewed and presented information on the privacy policies for some emerging technology vendors operating in Maryland. In addition, emerging technology vendors made presentations to the Council. Overall, the Council found privacy policies lacking and that the presenting vendors had a limited understanding of student data privacy laws. The vendors made generalized statements about data privacy, however they provided limited information on how their companies protect student data. Only one of the three emerging technology vendors had updated its policies to comply with national standards regarding student privacy issues.

Current environment and the impact of the Coronavirus Pandemic

After a robust discussion on the impact of the coronavirus pandemic on student data privacy, the Council concluded that Maryland's Student Data Privacy Act is applicable to emerging technologies

being implemented in the current environment. Council members discussed the need for appropriate training and professional development as an ongoing concern to ensure any technology implemented is used appropriately to protect student privacy. Members also discussed the privacy and security risks associated with distance learning and digital learning platforms.

Guiding Questions 7 and 8 Supporting Information:

Meeting Agenda	Agenda Item(s) and Presenter	Meeting Minutes
April 9, 2020	• Student Privacy and Coronavirus, Council Members • Emerging Technologies, Val Emrich, Director Instructional Technologies, MSDE	Minutes

Recommendations

Council Priorities

The Council established priorities to consider when developing final recommendations for this report. The Council developed the priorities based on the purpose and charge of the Council and on the information provided during meetings. These priorities are:

1. Alignment to the scope of the Student Data Privacy Act of 2015 (HB 298) and the Student Data Privacy Council Act (HB 245);
2. Ensure the protection of covered information used by Operators in Maryland's local school systems;
3. Ensure all stakeholders (Operators and local school systems) understand their roles under the Student Data Privacy Act of 2015;
4. Ensure flexibility across local school systems in the implementation of the Student Data Privacy Act of 2015.

Summary of Recommendations

The recommendations of the Council are presented in two sections: Statutory and Regulatory Changes and Continuation of the Council. Each recommendation includes relevant statute, if applicable, and a justification and rationale based on the findings of the Council.

1. Recommendations: Statutory and Regulatory
   1.1: Revise the meanings in the SDPA, Md. Ann. Code, Ed. Art. §4–131, to align to the Council developed and approved definitions.
   1.2A: Establish a mechanism(s) to ensure Operator compliance with the Student Data Privacy Act of 2015.
   1.2B: Ensure Operator breaches that violate the Student Data Privacy Act are subject to enforcement through the consumer protection law similar to the enforcement of violations under the Maryland Personal Information Protection Act.

1.3A: Require Operators to maintain a breach notification plan.

1.3B: Require public notification of violations of the Student Data Privacy Act.

2. Recommendations: Continuance of the Council

2.1: Repeal the Council's termination date to allow the Council to continue its evaluation of student data privacy in the State on a permanent basis.

2.2: Allow the Maryland Student Data Privacy Council to continue to meet periodically as determined by the Council Chair.

2.3: Revise the charge of the Maryland Student Data Privacy Council.

2.4: Require the Council to report on its revised charge on a periodic basis.

Recommendations: Statutory and Regulatory

1.1. Clarity

Revise the meanings in Md. Ann. Code, Ed. Art. §4–131 to align with the Council developed and approved definitions.

Justification and Rationale
In the review and analysis of similar laws and best practices in other states, the Council identified "clarity" as a best practice. The Council found during the study of the development and implementation of the SDPA that clearer language is necessary in defining Operators to ensure all stakeholders, including operators, understand the impact of the SDPA. The Council concluded that local school systems have the burden of ensuring that contracted operators comply with the Act. A subsequent survey of local school systems and review of the procurement processes in Maryland provided further confirmation that the onerous burden falls on local school systems to ensure that operators with whom they contract comply with the law. The Council determined the definition of "operator" was too limiting and expansion on the definition generated the majority of the discussion. Currently, the definition does not encompass non-educational, or general audience companies, as referenced on page 11 of this report. The definition also referred to an operator solely as "a person" and the Council decided adding the word 'entity' would make it comprehensive. One of the major changes recommended by the Council is that an entity that usually serves a general audience but has created a division for education clients would be considered the operator, and not the parent entity as a whole, so long as the education division does not share covered information with the parent entity. The definition for "covered information" was updated to include the definition of personally identifiable information and types of covered information were added or altered to the list, including online behavior or usage of applications when linked or linkable to a specific student. These changes resulted in less duplication and less confusion and the updated definition of covered information is referenced in two other revised definitions. The definition of a "persistent unique identifier" was edited significantly to extend coverage to a preK-12 student, their family, or a device linked to either party and not restrict the definition to simply a reference number. The updated definition of "targeted advertising" now incorporates the newly defined 'covered information' to replace online activities.

1.2. Compliance

A. Establish a mechanism(s) to ensure Operator's compliance with the Student Data Privacy Act of 2015.

Justification and Rationale
In study of the development and implementation of the SDPA, the Council noted the SDPA contains a lack of accountability and enforcement for operators. In the review and analysis of similar laws and best practices in other states, the Council identified "accountability" as a best practice and lacking in the SDPA. After presentations from local school system staff and analysis of local school system survey responses, the Council confirmed that the burden is on the local school systems for ensuring operators are compliant with the SDPA. Furthermore the local school system must mitigate issues at their own expense (both monetary and to student privacy). The establishment of a compliance mechanism would ensure operators comply with the SDPA and reduce the burden on local school systems. The Council discussed the following options to ensure compliance under the SDPA, including: 1. Utilize the same compliance process as the Maryland Personal Information Protection Act (MPIPA) to enforce the Student Data Privacy Act because it utilizes an already existing structure that enforces similar issues over similar entities. The decision makers involved in the process already have a specialized basis of knowledge. This option also helps ensure consistency in such matters throughout the State. 2. Establish a State Chief Privacy Officer with the authority and responsibility to address compliance and accountability of the SDPA. In the review of similar laws from other states, both Utah and New York, established similar roles and responsibilities. In addition to New York's chief privacy officer having the power to access all records and comment on the processing of student data, the law includes "any other powers that the commissioner shall deem appropriate." 3. Establish a new process for the Maryland State Department of Education or the Maryland Inspector General for Education to ensure compliance and accountability of operators as defined in the SDPA. These options are not ideal because both the MSDE and the Maryland Inspector General for Education have enforcement responsibilities over local school systems not operators as defined under SDPA.

B. Ensure Operator data breaches that violate the Student Data Privacy Act are subject to enforcement through the consumer protection law similar to the enforcement of violations under the Maryland Personal Information Protection Act.

Justification and Rationale
In study of the development and implementation of the SDPA, the Council noted the SDPA contains a lack of accountability and enforcement for operators around data breaches and unauthorized disclosure of student data. In the review and analysis of similar laws and best practices in other states, the Council identified that enforcement is lacking in the SDPA specific top data breaches. The local school systems, and students, who are impacted by a data breach must mitigate issues at their own expense (both monetary and to student privacy). The Council recommends using existing mechanisms

Justification and Rationale
to ensure that Operators data breaches that violate the Student Data Privacy Act are subject to enforcement to ensure compliance to the SDPA. The Council discussed the following options for enforcement: 1. Make sure Operator breaches under SDPA are subject to enforcement through the consumer protection law in the same way violations of Maryland Personal Information Protection Act are enforced through the consumer protection law. 2. Make the bridge between financial consumer records and student protected information clear to Operators.

1.3. Transparency

A. Require Operators to maintain a breach notification plan.

Justification and Rationale
In study of the development and implementation of the SDPA, the Council found that transparency and privacy are often at odds. In the review and analysis of similar laws and best practices in other states, the Council identified "accountability" as a best practice lacking in Maryland's SDPA. In their briefing on the Maryland Student Data Governance Act (HB0568, RS 2018), the Council learned that local school systems are required to develop and implement a breach notification plan, but that a similar requirement is lacking in the SDPA for Operators. Jackie La Fiandra, who provided advice to the Council from the Office of the Attorney General, clarified that businesses have requirements under the Maryland Personal Information Protection Act in response to breaches, but that based on MPIPA's definition of "personal information" those requirements do cover all of the data we traditionally view as education records (i.e. information on grades, State assessments, discipline, special education, etc…). The Council recommends expanding on the current requirements for operators under the law by adding a requirement to (C) (2) to include a breach notification plan to support more transparency and accountability of Operators. (c) An Operator shall: (2) implement and maintain reasonable security procedures and practices *including a breach notification plan* to protect covered information;

B. Require public notification of violations of the Student Data Privacy Act.

Justification and Rationale
In study of the development and implementation of the SDPA, the Council found that transparency and privacy are often at odds. Results from local school system implementation identified inconsistent practices across local school systems. Public notification of violations improves transparency and allows local school systems to identify potential issues with Operators prior to entering into contracts. In the review and analysis of similar laws and best practices in other states, the Council identified "accountability" as a best practice and lacking in the SDPA. Requiring public notification of violations of the SDPA supports both transparency and accountability.

Recommendations: Continuance of the Council

2.1. Repeal Termination

Repeal the termination date for the Council to allow the Council to continue its evaluation of student data privacy in the State on a permanent basis.

2.2. Continuance

The Maryland Student Data Privacy Council should continue to meet periodically as determined by the Council Chair.

Justification and Rationale
Continuance of the Council supports the best practices around "transparency" and "accountability". Emerging technology and changing practices due to the pandemic provide the opportunity for the Council to have a role in continuing to study the implementation of the SDPA and recommend changes as needed.

2.3. Charge

Revise the charge of the Maryland Student Data Privacy Council.

Justification and Rationale
The Council, as required, has studied the implementation of the SDPA. In light of the recommendations in this report, the Council recommends a change in the charge of the Council. The Maryland Student Data Privacy Council should: (1) Provide ongoing review and monitoring of the Act; (2) Review and analyze developments in technologies as they may relate to student data privacy; (3) Review the establishment and implementation of compliance mechanism(s) to determine its effectiveness in ensuring Operator's compliance with the Act. (4) Promote transparency on local school system contracted operators to families and the public.

Justification and Rationale
(5) Develop ways for local school systems to share information and expand communication among LSS on contracted Operators. (6) Review patterns of non-compliance with the Act.

2.4. Report

The Council shall report on their revised charge on a periodic basis.

Justification and Rationale
The Council shall report as needed to support the best practices around “transparency” and “accountability”. Emerging technology and changing practices due to the pandemic provide the opportunity for the Council to have a role in continuing to study the implementation of the SDPA and recommend changes as needed.

Maryland Student Data Privacy Council Members

One member of the Senate of Maryland, appointed by the President of the Senate:

- Susan C. Lee, Maryland Senate, District 16, Montgomery County
- Michael Lore (Designee), Chief of Staff, Senator Susan Lee

One member of the House of Delegates, appointed by the Speaker of the House:

- Jheanelle Wilkins, Maryland House of Delegates, District 20, Montgomery County (resigned)
- Dana Jones, Maryland House of Delegates, District 30A, Anne Arundel County

The State Superintendent of Schools, or the Superintendent's designee:

- Dr. Carol Williamson, Deputy Superintendent, Office of Teaching and Learning, Maryland State Department of Education

The Secretary of Information Technology, or the Secretary's designee:

- Chip Stewart, Acting Chief Information Security Officer
- Derek Wheeler (Designee), Assistant Director of Cybersecurity

The Executive Director of the Public School Superintendents' Association of Maryland, or the Executive Director's designee:

- Dr. Jeffrey Lawson, Superintendent of Cecil County Public Schools

The Executive Director of the Maryland Association of Boards of Education, or the Executive Director's designee:

- Michael Garman, MABE Member, Talbot County

The President of the Maryland State Education Association, or the President's designee:

- Chrystie Crawford-Smick, President, Harford County Education Association
- Samantha Zwerling (Designee), Government Relations Specialist, Maryland State Education Association

The President of the Maryland PTA, or the President's designee:

- Moisette "Tonya" Sweat, Vice President for Advocacy, Maryland PTA

One School Data Privacy Officer, or the Officer's designee:

- Theodore Hartman, Director of Strategy and Data Privacy, Howard County Public School System

One School Information Technology Officer, or the Officer's designee:

- Thomas Chapman, Assistant to Associate Superintendent, Office of Technology and Innovation, Montgomery County Public Schools

One representative of a company, trade association, or group who has professional experience in the area of student data privacy or online educational technology services:

- Michele McNeil, Vice President, Policy, The College Board

One member of the academic community who studies K–12 student data privacy:

- Dr. Ann Kellogg, Director of Reporting Services, Maryland Higher Education Commission, Maryland Longitudinal Data System Center

One advocate for student data privacy who does not have a professional relationship with a provider of online educational technology services:

- Baron Rodriguez, CEO, Noble Privacy Solutions LLC

One attorney who is knowledgeable in the laws and regulations that pertain to local school systems:

- Amelia Vance, Senior Counsel (Child Privacy) and Director of Education Privacy, Future of Privacy Forum

One school–based administrator from a public school in the State:

- Ryan Cowder, Worcester County Public Schools

One teacher from a public school in the State:

- Alison Vannoy, Anne Arundel Public Schools

The Maryland State Department of Education provided staff to the Council, including:

- Jackie C. La Fiandra, Assistant Attorney General, Office of the Attorney General
- Val Emrich, Director, Instructional Technology, School Library Media, and Mathematics, Division of Curriculum, Instructional Improvement and Professional Learning
- Chandra Haislet, Director, Accountability and Data Systems, Division of Assessment, Accountability and Information Technology
- Laia Tiderman, Program Manager, Accountability Support & Data Management, Accountability and Data Systems, Division of Assessment, Accountability and Information Technology
- Molly Abend, Data Management Coordinator, Accountability and Data Systems, Division of Assessment, Accountability and Information Technology, and Maryland Longitudinal Data System Center
- Shane McCormick, Executive Associate, Office of the Deputy for Teaching and Learning

Appendix

Relevant Definitions

ADDITIONS
[Removals]
Original text

Covered Information

- (A) (2) (i) "Covered information" means information or material 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.
  [1. personally identifies an individual student in this State or that is linked to information or material that personally identifies an individual student in this State; and 2. Is gathered by an operator through the operation of a site, a service, or an application.]
  (ii) "Covered information" includes but is not limited to a student's:
    1. Educational [and disciplinary] records as defined by Md. Code, Ed. Art., §7–1303;
    2. First and last name;
    3. Home address and geolocation information;
    4. Telephone number;
    5. Electronic mail address or other information that allows physical or online contact;
    6. Test results, grades, and student evaluations;
    7. Special education [data] information;
    8. Disciplinary information;
    [8]9. Criminal records;
    [9]10. Medical records and health records;
    [10]11. Social Security number;
    [11]12. Biometric information;
    [12]13. Socioeconomic information;
    [13]14. Food purchases;
    [14]15. Political and religious affiliations;
    [15]16. Text messages;
    [16]17. Student identifiers;
    [17]18. Search activity;
    19. Online behavior or usage of applications when linked or linkable to a specific student;
    [18]20. Photos; [and]
    [19]21. Voice recordings; and
    22. Persistent unique identifiers.

(iii)"Covered information" may also include confidential information as defined by the Maryland Department of Information Technology.

Operator

- (A) (3) "Operator" means a person or entity who is operating in accordance with a contract or an agreement with a PreK-12 public school or local school system in the State to provide an Internet web site, an online service, an online application, or a mobile application, that processes covered information and:
  (i) Is used [primarily] for a PreK–12 school purpose; or
  (ii) Is issued at the direction of a public school, a teacher, or any other employee of a public school, local school system, or the Department. [; and
  [(iii) Was designed and marketed primarily for a PreK–12 school purpose.]

  Operator is only intended to apply when organizations engage with institutions under FERPA's School Official exception. Other exceptions apply, namely Audit/Evaluation and the Studies Exception, which is still subject to FERPA's "reasonable methods" and associated contractual privacy and security safeguards.

  If an entity usually serves a general audience but has created a division for education clients, that division will be considered the entity covered by this law, and not the parent entity as a whole, so long as the education division does not share covered information with the parent entity.

Persistent Unique Identifier

- (A) (4) "Persistent unique identifier" means an identifier that can be used to identify, recognize, track, single out, or make inferences about a preK-12 student, their family, or a device that is linked to a preK-12 student or family, over time and across services, including, but not limited to, a device identifier; a cookie identifier, mobile ad identifiers, or similar technology; customer number, unique pseudonym, hashed email address, hashed phone number, or other user alias; including identifiers generated through probabilistic methods. For purposes of this definition, "family" means a custodial parent or guardian and any preK-12 students over which the parent or guardian has custody. [a unique reference number used as an identifier in computer software that is stored across different usage sessions]

PreK–12 school purpose (No Changes)

- (A) (5) (i) "PreK–12 school purpose" means an activity that:
  1. Takes place at the direction of a public school, a teacher, an administrator, or a local school system; or
  2. Aids in the administration of public school activities.

  (ii) "PreK–12 school purpose" includes:
  1. Instruction in the classroom;
  2. Home instruction;

3. Administrative activities;
4. Collaboration among students, public school employees, and parents;
5. Maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application; and
6. An activity that is for the use and benefit of the public school.

Targeted Advertising

- (A) (6) (i) "Targeted advertising" means presenting advertisements to an individual student that are selected based on information obtained or inferred from the student's [online behavior, usage of applications, or] covered information.
  (ii) "Targeted advertising" does not include advertisements presented to an individual student at an online location:
  1. Based on the student's current visit to the online location [without] so long as there is no collection or retention of the student's [online activities] covered information over time; or
  2. In response to a single search query [without] so long as there is no collection or retention of the student's covered information [online activities] over time.