

SB 733 - Education – Student Data Privacy – Report

Uploaded by: Zwerling, Samantha

Position: FAV

Testimony in SUPPORT of Senate Bill 733
Education – Student Data Privacy – Reports and Student Data Privacy Council Sunset Extension

Senate Education, Health, and Environmental Affairs Committee
March 9, 2021

Samantha Zwerling
Government Relations

The Maryland State Education Association supports SB 733, legislation that originated in the Student Data Privacy Council and aims to help protect student data. .

MSEA represents 75,000 educators and school employees who work in Maryland’s public schools, teaching and preparing our 896,837 students for careers and jobs of the future. MSEA also represents 39 local affiliates in every county across the state of Maryland, and our parent affiliate is the 3 million-member National Education Association (NEA).

MSEA is proud to serve on the Student Data Privacy Council and hopes to continue, should this bill and the Council’s extension of service be passed into law. MSEA agrees that we must do all we can to ensure to protect student and educator data in all forms. This bill expands the coverage of what would be deemed confidential information, in an effort to protect students from identity fraud and theft as well making them vulnerable to intrusive marketing.

MSEA looks forward to further discussions on vetting online tools in a systemic way, while also maintaining educator autonomy in determining which tools are best for their students. The extension of the Council’s work will allow for conversations on this topic.

MSEA urges a favorable report of Senate Bill 733.

Lee_FAV_SB733_2021.pdf

Uploaded by: Lee, Susan

Position: FWA

SUSAN C. LEE
Legislative District 16
Montgomery County

MAJORITY WHIP

Judicial Proceedings Committee

Joint Committee on
Cybersecurity, Information Technology,
and Biotechnology

Chair Emeritus
Maryland Legislative Asian American
and Pacific Islander Caucus

President Emeritus
Women Legislators of the
Maryland General Assembly, Inc.



James Senate Office Building
11 Bladen Street, Room 223
Annapolis, Maryland 21401
410-841-3124 • 301-858-3124
800-492-7122 Ext. 3124
Susan.Lee@senate.state.md.us

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

March 9, 2021

Senate Education, Health, and Environmental Affairs Committee

**Senate Bill 733 - Education - Student Data Privacy - Reports and Student
Data Privacy Council Sunset Extension**

This is legislation that has combined two common sense measures. The first is a codification of the report and findings from the Student Data Privacy Council. I encourage you to view this link to the final [Student Data Privacy Council Report](#). The second measure is a reporting requirement that the local school systems pass along a simple list of digital education tools that are either approved, prohibited, or a third category of used but not yet formally approved. The reporting requirement provision was supported separately as a stand-alone recommendation from the Maryland Joint Committee on Cybersecurity, Information Technology and Biotechnology.

We sent the request to drafters to codify the recommendations of the Council report, and while there appear to be some minor inconsistencies, we defer to the Final Council language as much as possible. The update of definitions include ensuring there isn't a backdoor connection to the personal identifying information to be sold to third parties, and expands the list of protected categories. The scope of the Council was very narrowly focused on the Student Data Privacy Act, so the recommendations do not extend beyond the charge of the body, however, I felt it was important to include a reporting mechanism on digital education tools across all 24 jurisdictions.

This simple measure would require MSDE to post the information as provided by the local school systems. This is not a mandate beyond reporting the digital education tool status so parents have a resource to decipher what is approved, and what is not approved in their LSS, and perhaps what other counties are doing in this space, so they can push for best practices.

For these reasons, I respectfully request a favorable committee report on SB 733, as amended.

SB 733.Student Dat Privacy Act Revisions.pdf

Uploaded by: Woolums, John

Position: FWA

BILL: Senate Bill 733
TITLE:
DATE: March 9, 2021
POSITION: SUPPORT WITH AMENDMENTS
COMMITTEE: Education, Health, and Environmental Affairs
CONTACT: John R. Woolums, Esq.

The Maryland Association of Boards of Education (MABE) supports Senate Bill 733 to the extent it is consistent with the final recommendations of the Student Data Privacy Council, but not to the extent that it includes provisions expanding those recommendations to impose additional requirements on local school systems. Specifically, MABE does not support the bill provisions to mandate the identification and posting of all approved, disapproved, and known digital tools.

MABE strongly supported the General Assembly's initiative to establish the Student Data Privacy Council responsible for studying and making recommendations regarding the development and implementation of the Student Data Privacy Act of 2015. MABE supports Senate Bill 733 to the full extent that it reflects the Council's work under the Student Data Privacy Act and its final report of January 13, 2021. These adopted recommendations include the following:

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.

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.

MABE supports these recommendations and the work of the Council to address the serious and ongoing policy area involving the use by students, teachers, and school systems of online information and educational tools. The attention to the issue in local school systems in Maryland and across the nation is driven by the awareness of the need to adopt school system policies, contract language, and state laws, in order to protect student privacy while using online educational services. MABE believes that extending the sunset provision for Student Data Privacy Council will help to ensure statewide implementation of security measures to prevent unauthorized access, destruction, use, modification, or disclosure of information gathered based on students' computer usage.

For these reasons, MABE requests a favorable report on Senate Bill 733 with the amendments described above.

AACPS SB733 Data Privacy OPP 3.9.21.pdf

Uploaded by: Ortiz, Jeanette

Position: UNF



**SB733 EDUCATION - STUDENT DATA PRIVACY - REPORTS AND STUDENT DATA PRIVACY
COUNCIL SUNSET EXTENSION**

March 9, 2021

EDUCATION, HEALTH, AND ENVIRONMENTAL AFFAIRS COMMITTEE

OPPOSE

Jeanette Ortiz, Esq., Legislative & Policy Counsel (410.703.5352)

Anne Arundel County Public Schools (AACPS) opposes **SB733 Education - Student Data Privacy - Reports and Student Data Privacy Council Sunset Extension**. This bill requires each county board of education to provide a list of digital tools to MSDE on or before July 1 each year. It also requires MSDE to publish information on digital tools provided by each county board on or before September 1 each year. The bill requires the Student Data Privacy Council to submit a report to the Governor and the General Assembly on or before December 1, 2024, and it extends the termination date for the Council to September 30, 2025.

AACPS does not believe that this legislation is necessary as student privacy is currently covered under the Family Educational Rights and Privacy Act (FERPA) and local school systems must comply with all the provisions outlined in the federal law. As such, there is no real purpose to the additions proposed in this bill which would simply create additional work and result in workload issues for a local school system. It is unclear how an online dashboard listing all digital tools that students and schools use helps with the implementation of FERPA or how this helps to further protect student privacy local school systems are already required to protect. The term “digital tools” is not defined. Another concern is that the legislation requires local school systems to report digital tools that are “not authorized” by the county board of education. First, it is important to note that whether or not to authorize specific digital tools is actually a decision that would be made by a local superintendent as part of the superintendent’s authority and responsibility in running the daily operations of a school system. Second, it is unclear how a local school system would report on digital tools that are “not authorized” if the school system is not aware of every potential digital tool available. The number of potential digital tools available to a local school system is extensive and there is just no reasonable expectation for a school system to be cognizant of every single potential digital tool and determine which digital tools are not authorized.

It is also important to note that digital tools are constantly evolving, and school systems use numerous digital tools in teaching and learning. In fact, AACPS has a comprehensive approval process regarding materials of instruction, which includes digital tools. This process includes specific criteria in our vendor agreements that address student data privacy. Again, this process exists now as a result of FERPA.

It is also important to note that this bill goes above and beyond recent recommendations by the Student Data Privacy Council. Also, the General Assembly passed legislation in recent years addressing the protection and disclosure of student data as well as legislation requiring MSDE develop best practices concerning data governance. As a result of these recent laws, school systems have developed policies and procedures to implement such best practices.

Accordingly, AACPS respectfully requests an **UNFAVORABLE** committee report on SB733.

SB0733 - MCPS-UNFAV.pdf

Uploaded by: Susskind, Danielle

Position: UNF



MONTGOMERY COUNTY BOARD OF EDUCATION

Expanding Opportunity and Unleashing Potential

850 Hungerford Drive ♦ Room 123 ♦ Rockville, Maryland 20850

BILL: SB0733 (Cross filed with HB1062)
TITLE: Education - Student Data Privacy - Reports and Student Data Privacy
Council Sunset Extension
DATE: 3/9/2021
POSITION: Oppose
COMMITTEE: Education, Health, and Environmental Affairs
CONTACT: Danielle M. Susskind, Coordinator, Legislative Affairs
[Danielle M Susskind @mcpsmd.org](mailto:Danielle_M_Susskind@mcpsmd.org)

The Montgomery County Board of Education (Board) **opposes** SB0733.

- Bill proposes revisions to clarify/expand the definition of student information covered by student data privacy
- Defines “persistent Unique Identifiers, and
- Requests that each County submit an annual list of digital tools, including:
 - Approved Digital Tools
 - Digital Tools known to be used by educators
 - Digital tools not authorized by the County Board

The decision on which digital tools are used in the education process is not made at specific intervals during the year, but instead is made on an as-needed basis. Tools are added constantly. Montgomery County Public Schools (MCPS) already publishes all approved and not-approved sites on its website. When requests are made to use digital tools at MCPS, they are thoroughly vetted to ensure the tools adhere to our safety and security guidelines. The either receive an approved, requires affirmative parental consent, or not-approved ratings. Here is more information: <https://www.montgomeryschoolsmd.org/data-privacy-security/>.

For these reasons, the Board **opposes** this legislation and urges an unfavorable report.

SB 733 Student Data Privacy INFO PSSAM Cecil Co PS

Uploaded by: Fannon, Mary Pat

Position: INFO



Bill: SB 733 – Education – Student Data Privacy – Reports and Student Data Privacy Council Sunset Extension

Date: March 9, 2021

Position: Letter of Information

Committee: Senate Education, Health and Environmental Affairs

Contact: Mary Pat Fannon, Executive Director, PSSAM
Jeffrey A. Lawson, Ed.D., Cecil County Public Schools

This legislation requires each county board of education to provide a certain list of digital tools to the State Department of Education on or before July 1 each year; requires the Department to publish certain information on digital tools provided by each county board; requires the Student Data Privacy Council to submit a report to the Governor and the General Assembly on or before December 1, 2024; and, extends the termination date for the Council to September 30, 2025.

The Public Schools Superintendents' Association of Maryland (PSSAM) and Dr. Jeffrey Lawson, in his capacity as the PSSAM representative to the Council, provide this letter of information regarding Senate Bill 733.

The Student Data Privacy Council met as required through 2020 and concluded with a set of recommendations in its final report. The Council concluded that the Student Data Privacy Act had been implemented as intended and provided suggestions in terms of additional clarification and other potential adjustments that could improve the Act's successful implementation. While much of the conversation focused on operators (those third-party vendors who serve Local School Systems [LSS]), there was considerable discussion surrounding the ability of LSSs to ensure compliance on the part of these operators. Moreover, there was also concern about the ability and internal capacity of each LSS to monitor the many operators due to the differences in operations and guidelines among systems.

While this bill incorporates some of the Council's recommendations and extends the Council's termination date, there are some concerning elements for LSSs and our chief information officers. Some of the bill's requirements go further than the Council's recommendations and creates duplicative work for school systems. Specifically, the bill requests student privacy information that is already covered by federal law (FERPA) and each LSS complies with all federal provisions. In addition, the proposed legislation requires LSSs to report digital tools "not authorized" by the county board. Currently, when LSSs discover unauthorized digital tools, we are required to stop using them. Lastly, digital tools constantly change and there are hundreds in use across the state for teaching & learning. Approval of these tools includes extensive student privacy criteria reflected in agreements with vendors. Gathering and reporting all of the tools and operators in use, and providing documentation to the MSDE will be costly and logistically challenging.

Therefore, we respectfully ask the committee to consider these points in your deliberations and to focus on the Council's recommendations and the extension of the Council's work that are incorporated in the bill.

Mary Pat Fannon, marypat.fannon@pssam.org
410-935-7281

Dr. Jeffrey Lawson, jlawson@ccps.org
410-996-1040

SIIA Written Testimony MD SB 733.pdf

Uploaded by: Kloek, Sara

Position: INFO



**Written Testimony
Sara Kloeck
Senior Director, Education Policy
Software & Information Industry Association**

**SENATE EDUCATION, HEALTH & ENVIRONMENTAL AFFAIRS COMMITTEE
Bill Hearing: SB 733 (Education - Student Data Privacy - Reports and Student Data
Privacy Council Sunset Extension)**

March 9, 2021

Thank you for holding this important hearing. The Software & Information Industry Association (SIIA) is pleased to offer testimony on SB 733.

SIIA is a professional organization connecting more than 700 financial information, education technology, specialized content and publishing, and health technology companies. Our education technology membership develops and delivers software applications, digital instructional content, online and distance learning services, online assessment, and related technologies for millions of learners across the nation. Our members are dedicated to partnering with educators and schools across the country to improve student outcomes while protecting student privacy.

Maryland is a leader in that the establishment and work product of the Student Data Privacy Council, with representation from a diverse number of stakeholders, offers the state a perspective like no other state has on student data privacy. The Student Data Privacy Council's report should play an important role in the development of practices at the school level as well as possible amendments to the state's student privacy laws.

We are concerned that some of the language in SB 733 does not align with the Student Data Privacy Council report and that some of the requirements may place an undue burden on schools without additional resources and guidance. We urge the committee to

consider a few amendments to the text that would help align the bill to the report and strengthen protections for student privacy in Maryland.

- The proposed language could expand the scope of the law to cover non-education services that are not intended for use in schools. These non-education services would have no knowledge they are being used in schools nor subject to the law. We support maintaining the second prong of the definition of operator so that a mere recommendation by teacher or employee of a school will not make an entity an operator. In addition to keeping the connection with the school, we recommend deleting the word “purpose” so that the scope is narrowed
- We support language in the definition of persistent unique identifier to clarify that it is a unique identifier stored across usage sessions. Without putting this language back into the definition, it simply is not persistent.
- We continue to support the existence and work of the Student Data Privacy Council. We are concerned that the requirement for county boards to submit lists of approved, known, and not authorized digital tools to the Department comes without funding or guidance. We are also concerned that there is no clear process for getting added as an approved digital tool or being listed as a digital tool that is not authorized by the county board. Instead, SIIA encourages the removal of this provision and adding new requirements for the Student Data Privacy Council’s 2024 report that would help establish best practices for school privacy programs.

Suggested amendment language is included below. Thank you for your time.

Respectfully,

Sara Kloek
Senior Director, Education Policy
Software & Information Industry Association

Suggested Amendments

Software & Information Industry Association

Sara Kloek

Senior Director, Education Policy

skloek@siia.net

A BILL ENTITLED

1 AN ACT concerning

Education – Student Data Privacy – Reports and Student Data Privacy Council

2 **Sunset Extension**

3 FOR the purpose of requiring each county board of education to provide a
4 certain list of

5 digital tools to the State Department of Education on or before a certain
6 date each

7 year; requiring the Department to publish certain information on digital
8 tools

9 provided by each county board on or before a certain date each year;
10 requiring the

11 Student Data Privacy Council to submit a certain report to the Governor
12 and the

13 General Assembly on or before a certain date; extending the termination date
14 for the

15 Council; altering certain definitions; and generally relating to student data
16 privacy

in the State.

11 BY repealing and reenacting, with amendments,

12 Article – Education

13 Section 4–131(a)

14 Annotated Code of Maryland

15 (2018 Replacement Volume and 2020 Supplement)

16 BY adding to

17 Article – Education
18 Section 4–131(p)
19 Annotated Code of Maryland
20 (2018 Replacement Volume and 2020 Supplement)

21 BY repealing and reenacting, with amendments,
22 Chapter 398 of the Acts of the General Assembly of 2019
23 Section 1(h) and 2

24 SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,
25 That the Laws of Maryland read as follows:

1 Article – Education

2 4–131.

3 (a) (1) In this section the following words have the meanings indicated.

4 (2) (i) “Covered information” means information or material that[:

5 1. Personally identifies an individual student in this State or
6 that is linked to information or material that personally identifies an individual student in
7 this State; and

8 2. Is gathered by an operator through the operation of a site,
9 a service, or an application],

**ALONE OR IN COMBINATION WITH OTHER INFORMATION OR MATERIAL, IS LINKED OR COULD BE LINKED
TO A STUDENT IN A MANNER THAT WOULD ALLOW AN EMPLOYEE OR STUDENT OF THE STUDENT'S
SCHOOL TO IDENTIFY THE STUDENT WITH REASONABLE CERTAINTY.**

10 (ii) “Covered information” includes a student’s:

11 1. Educational [and disciplinary record] **RECORDS AS**
12 **DEFINED IN § 7–1303 OF THIS ARTICLE;**

13 2. First and last name;

14 3. Home address and geolocation information;

15 4. Telephone number;

16 5. Electronic mail address or other information that allows
17 physical or online contact;

18 6. Test results, grades, and student evaluations;

19 7. Special education [data] **INFORMATION;**

20 8. Criminal records;

21 9. Medical records and health records;

22 10. Social Security number;

23 11. Biometric information;

24 12. Socioeconomic information;

- 13. Food purchases;
- 14. Political and religious affiliations;
- 15. Text messages;
- 16. Student identifiers;
- 17. Search activity;
- 18. Photos; [and]
- 19. Voice recordings;

20. DISCIPLINARY INFORMATION;

**21. ONLINE BEHAVIOR OR USAGE OF APPLICATIONS
WHEN LINKED OR LINKABLE TO A SPECIFIC STUDENT;**

22. PERSISTENT UNIQUE IDENTIFIERS; AND

**23. CONFIDENTIAL INFORMATION AS DEFINED BY THE
DEPARTMENT OF INFORMATION TECHNOLOGY.**

(3) “Operator” means [a person] **AN INDIVIDUAL OR AN ENTITY** 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 website, an online service, an online application, or a mobile application that:

(i) PROCESSES COVERED INFORMATION; AND

- OR**
- [(i)] (ii) 1.** Is used [primarily]–for a PreK–12 school purpose;
 - [(ii)] 2.** 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 schools. [purpose].

(4) **(i)** “Persistent unique identifier” means [a unique referencenumber used as an identifier in computer software that is stored across different usage sessions] **AN IDENTIFIER THAT IS USED TO IDENTIFY, RECOGNIZE, TRACK, SINGLE OUT,**

28 OR MAKE REFERENCES ABOUT A STUDENT ENROLLED IN PREKINDERGARTEN
29 THROUGH GRADE 12, THE PARENT OR GUARDIAN OF THE STUDENT, AND ANY OTHER

1 STUDENT OF WHOM THE PARENT OR GUARDIAN HAS CUSTODY **THAT IS STORED ACROSS USAGE**
2 **SESSIONS.**

2 (ii) **“PERSISTENT UNIQUE IDENTIFIER” INCLUDES:**

- 3 1. **COOKIE IDENTIFIERS;**
- 4 2. **CUSTOMER NUMBERS;**
- 5 3. **DEVICE IDENTIFIERS;**
- 6 4. **HASHED E—MAIL ADDRESSES;**
- 7 5. **HASHED PHONE NUMBERS;**
- 8 6. **IDENTIFIERS GENERATED THROUGH PROBABILISTIC**
9 **METHODS;**
- 10 7. **MOBILE AD IDENTIFIERS;**
- 11 8. **UNIQUE PSEUDONYMS; AND**
- 12 9. **USER ALIASES.**

13 (5) (i) **“PreK–12 school purpose” means an activity that:**

- 14 1. Takes place at the direction of a public school, a teacher,
15 an administrator, or a local school system; or
- 16 2. Aids in the administration of public school activities.

17 (ii) **“PreK–12 school purpose” includes:**

- 18 1. Instruction in the classroom;
- 19 2. Home instruction;
- 20 3. Administrative activities;
- 21 4. Collaboration among students, public school employees,
22 and parents;
- 23 5. Maintaining, developing, supporting, improving, or
24 diagnosing the operator’s site, service, or application; and

6. An activity that is for the use and benefit of the public

1 school.

2 (6) (i) "Targeted advertising" means presenting advertisements to an
3 individual student that are selected based on information obtained or inferred from the
4 student's [online behavior, usage of applications, or]covered information.

5 (ii) "Targeted advertising" does not include advertisements
6 presented to an individual student at an online location:

7 1. Based on the student's current visit to the online location
8 [without] IF THERE IS NO collection or retention of the student's [online activities]
9 COVERED INFORMATION over time; or

10 2. In response to a single search query [without] IF THERE
11 IS NO collection or retention of the student's [online activities] COVERED INFORMATION
12 over time.

13 [(P) (1) ON OR BEFORE JULY 1, 2021, AND EACH JULY 1 THEREAFTER,
14 EACH COUNTY BOARD SHALL SUBMIT TO THE DEPARTMENT A LIST OF THE
15 FOLLOWING DIGITAL TOOLS WITH RESPECT TO THE IMMEDIATELY PRECEDING
16 SCHOOL YEAR:

17 (i) APPROVED DIGITAL TOOLS;

18 (ii) DIGITAL TOOLS KNOWN TO BE USED BY EDUCATORS; AND

19

20 (iii) DIGITAL TOOLS NOT AUTHORIZED BY THE COUNTY BOARD.

21 (2) ON OR BEFORE SEPTEMBER 1, 2021, AND EACH SEPTEMBER 1
22 THEREAFTER, THE DEPARTMENT SHALL PUBLISH AN ONLINE DATABASE OF THE
23 DIGITAL TOOLS REPORTED BY EACH COUNTY BOARD IN ACCORDANCE WITH
24 PARAGRAPH (1) OF THIS SUBSECTION.]

24 Chapter 398 of the Acts of 2019

25 SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,
26 That:

27 (h) (1) On or before December 31, 2020, the Student Data Privacy Council
28 shall report its findings and recommendations to the Governor and, in accordance with §
29 2-1246 of the State Government Article, the General Assembly.

30 (2) ON OR BEFORE DECEMBER 1, 2024, THE STUDENT DATA

31 **PRIVACY COUNCIL SHALL REPORT TO THE GOVERNOR AND, IN ACCORDANCE WITH**
32 **§ 2-1257 OF THE STATE GOVERNMENT ARTICLE, THE GENERAL ASSEMBLY ON:**

1 [(I) THE IMPLEMENTATION OF § 4-131(P) OF THE EDUCATION
2 ARTICLE;
AND]

3 (I) BEST PRACTICES FOR STUDENT DATA PRIVACY
4 PROTECTION TO PROVIDE TO PARENTS AND GUARDIANS OF STUDENTS IN THE
5 STATE;

6 (II) BEST PRACTICES FOR DEVELOPING TRANSPARENT STUDENT PRIVACY
PROGRAMS AT THE SCHOOL AND/OR COUNTY LEVEL; AND

7 (III) BEST PRACTICES FOR COMMUNICATING ABOUT STUDENT DATA PRIVACY
PROGRAMS AT THE SCHOOL AND/OR COUNTY LEVEL.

8 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect June
9 1, 2019. It shall remain in effect for a period of [2] 6 years and 4 MONTHS AND, at the end
10 of [May 31, 2021] SEPTEMBER 30, 2025, this Act, with no further action required by the
11 General Assembly, shall be abrogated and of no further force and effect.

12 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect June 11 1,
2021.