The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Rules

BILL:	SB 662
INTRODUCER:	Senator Bradley
SUBJECT:	Student Online Personal Information Protection
DATE:	April 4, 2023
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Collazo	Cibula	JU	**Favorable**
2.	Brick	Bouck	ED	**Favorable**
3.	Collazo	Twogood	RC	**Pre-meeting**

I. Summary:

SB 662 creates the Student Online Personal Information Protection Act, which substantially restricts the operator of a website, online service, or online application that is used for K-12 school purposes from collecting, disclosing, or selling student data, or from using student data to engage in targeted advertising.

The bill prohibits operators from knowingly:

- Engaging in targeted advertising based on any information, including persistent unique identifiers, acquired through the use of their educational technology.
- Using any information, including persistent unique identifiers, gathered through their educational technology to create profiles of students, except for K-12 school purposes.
- Sharing, selling, or renting student information to third parties.
- Disclosing certain covered information, except under specified circumstances.

The bill requires operators to:

- Collect no more covered information than reasonably necessary to operate the educational technology.
- Implement and maintain reasonable security procedures and practices to protect covered information.
- Delete a student's covered information if requested by the K-12 school or school district, unless a student or a parent or guardian consents to its maintenance.

The bill allows operators to disclose covered information if:

- Federal or state law requires disclosure.
- It is disclosed for legitimate research purposes, if not used for targeted advertising or profiling for purposes other than K-12 school purposes.

- It is disclosed to a state or local educational agency, including K-12 schools and school districts, for K-12 school purposes.

The bill takes effect July 1, 2023.

II. Present Situation:

Privacy of Student Information

Since the pandemic, schools have significantly increased their reliance upon Internet and online-based software and educational technologies. Classroom assignments and assessments are often delivered online via laptops or tablets, and teachers make regular use social media platforms, websites, and "free" apps in class.[1] In fact, a single educator will use, on average, 148 apps in a school year.[2] This increased reliance on Internet-based apps in schools risks compromising student privacy because it exposes students to online profiling and targeted advertising.

Profiling is the automated process of compiling personal data to evaluate certain personal aspects relating to a specific student.[3] The operators of Internet-based apps can use persistent unique identifiers or third-party scripts to recognize and track students across third-party websites, then use this information to analyze or predict student interests for marketing or advertising purposes. Tracking students in this manner can result in unintended consequences such as the disclosure of sensitive data through unknown tracking processes.[4]

Targeted advertising collects generalized information about students from various sources, including their race, location, gender, age, school, or interests.[5] This information is then interpreted in order to display products and services that may be more relevant (i.e. targeted) to students. Targeted advertising can also include the collection of specific information about individual students using cookies, beacons, tracking pixels, persistent unique identifiers, or other tracking technologies that provide more specific information about a student's online behavior or activities over time. This information can then be sold to, or shared with, third-party advertisers, who are able to display even more targeted products and services to students than general targeted advertisements based on the highly-specific information they received from the student's behavior while using the application or service.[6]

Targeted advertising is different than contextual advertising, which displays products and services to students based only on the content or webpage that they are currently viewing, and

---

[1] Parent Coalition for Student Privacy and the Network for Public Education, *The State Student Privacy Report Card: Grading the States on Protecting Student Data Privacy*, 1 (Jan. 2019), https://studentprivacymatters.org/wp-content/uploads/2019/01/The-2019-State-Student-Privacy-Report-Card.pdf.
[2] Rebecca Torchia, *What is Third-Party Risk, and What Do Schools Need to Know?* (Feb. 24, 2023), EdTech Focus On K-12, https://edtechmagazine.com/k12/article/2023/02/what-third-party-risk-and-what-do-schools-need-know-perfcon (citing LearnPlatform, *EdTech Top 40: Fall Report* (Sept. 2022), https://learnplatform.com/top40).
[3] Girard Kelly, *How California's Student Privacy Law Protects Against Targeted Advertising* (Apr. 26, 2018), The Journal, https://thejournal.com/articles/2018/04/26/how-california-student-privacy-law-protects-against-targeted-advertising.aspx.
[4] *Id.*
[5] *Id.*
[6] *Id.; see also* Wharton School, University of Pennsylvania, *Your Data Is Shared and Sold… What's Being Done About It?* (Oct. 28, 2019), Knowledge at Wharton, https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/.

which does not collect any specific information about the student to determine which advertisements to display.[7]

There is significant unease about the privacy implications associated with the online collection and use of data.[8] One international, pre-pandemic poll found that 71% of individuals worried about how tech companies collect and use their personal data.[9] And in another poll, specifically with respect to the collection and use of K-12 student data, 93% of parents of K-12 students said it was important for schools to engage with them about the use of student data, but only 44% said that they had been asked for their input.[10]

State Student Privacy Legislation

At the state level, 42 states and the District of Columbia have passed more than 128 student privacy laws.[11] Indeed, most states have passed more than one student privacy law.[12]

States have generally approached the regulation of student data use in three ways:
- By regulating schools and state-level education agencies;
- By regulating companies that collect and use student data; and
- By combining the first two models.[13]

An example of the first approach is Oklahoma's Student Data Accessibility, Transparency, and Accountability Act of 2013 (the Student DATA Act), which addressed the permissible state-level collection, security, access, and uses of student data. Legislation following the Oklahoma model has limited data collection and use and defined how holders of student data can collect, safeguard, use, and grant access to data.[14]

An example of the second approach is California's Student Online Personal Information Protection Act (SOPIPA), which prevents online service providers from using student data for commercial purposes, while allowing specific beneficial uses such as personalized learning.

---

[7] Kelly, *supra* at note 3.
[8] *See* University of Texas at Austin, Center for Media Engagement, *Privacy versus Products in Targeted Digital Advertising*, https://mediaengagement.org/research/privacy-versus-products-in-targeted-digital-advertising/ (last visited Feb. 28, 2023).
[9] Amnesty International, *New poll reveals 7 in 10 people want governments to regulate Big Tech over personal data fears* (Dec. 4, 2019), https://www.amnesty.org/en/latest/press-release/2019/12/big-tech-privacy-poll-shows-people-worried/.
[10] Adam Stone, *Understanding FERPA, CIPA, and Other K-12 Student Data Privacy Laws* (Apr. 28, 2022), EdTech Focus On K-12, https://edtechmagazine.com/k12/article/2022/04/understanding-ferpa-cipa-and-other-k-12-student-data-privacy-laws-perfcon (citing the Center for Democracy and Technology, *Sharing Student Data Across Public Sectors* (Dec. 2021), *available at* https://cdt.org/wp-content/uploads/2021/12/12-01-2021-Civic-Tech-Community-Engagement-Full-Report-final.pdf).
[11] *Id.* (citing a senior technologist with at the Future of Privacy Forum at https://fpf.org/).
[12] LearnPlatform, *Student Data Privacy Regulations Across the U.S.: A Look at How Minnesota, California and Others Handle Privacy*, https://learnplatform.com/blog/edtech-management/student-data-privacy-regulations (last visited Feb. 28, 2023); *see also* Student Privacy Compass, *State Student Privacy Laws*, https://studentprivacycompass.org/state-laws/ (last visited Feb. 28, 2023) (maintaining a running list of state student privacy laws).
[13] The Student Privacy Compass, *Policymakers: Student [State] Laws and Legislation*, https://studentprivacycompass.org/audiences/policymakers/ (last visited Feb. 27, 2023).
[14] *Id.*; *see also* State of Oklahoma, Department of Education, *Data Privacy and Security*, https://sde.ok.gov/data-privacy-and-security (last visited Feb. 28, 2023) (describing, among other things, certain important provisions of the Student DATA Act of 2013).

California supplemented SOPIPA by enacting AB 1584, a law that explicitly allows districts and schools to contract with third parties in order to manage, store, access, and use information in students' education records. An enforcement provision, AB 375, was also added to give the California Attorney General additional authority to fine companies that violate SOPIPA and AB 1584. This law has become a model for the regulation of educational technology vendors' use of student data; more than 20 states have since adopted similar laws.[15]

Examples of the third approach may be found in Georgia and Utah:

- To regulate its state longitudinal data system,[16] Georgia chose to follow Oklahoma's lead in addressing three core issues regarding state education entities: which data is collected, how student data can be used securely and ethically, and who can access student data. Combined with SOPIPA-like regulation of third parties, this approach has allowed innovative uses of student data while establishing meaningful privacy protections for students.[17]
- Similarly, Utah has taken a modified hybrid approach by regulating districts, the state education agency, and companies. Utah took the additional step of creating and funding a Chief Privacy Officer and three additional privacy staff not only to carry out the law, but also to provide training for teachers and administrators and to create resources that help stakeholders ensure compliance.[18]

Since 2015, state legislation has tended to regulate data use rather than collection, and to focus laws on specific privacy topics such as data deletion, data misuse, biometric data, and breach notification.[19]

Federal Student Privacy Legislation

At the federal level, there are three laws that are most often referenced when it comes to student privacy and local schools or school districts:[20] the Family Educational Rights and Privacy Act,[21] the Protection of Pupil Rights Amendment,[22] and the Children's Online Privacy Protection Act (COPPA).[23]

---

[15] The Student Privacy Compass, *supra* note 13; *see also* State of California, Department of Justice, *Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data*, 7-9 (Nov. 2016), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/ready-for-school-1116.pdf (describing, among other things, SOPIPA's provisions).

[16] In education, a longitudinal data system is a data system that collects and maintains detailed, high quality, student- and staff-level data; links these data across entities and over time, providing a complete academic and performance history for each student; and makes these data accessible through reporting and analysis tools. National Center for Education Statistics, U.S. Department of Education, *Traveling Through Time: The Forum Guide to Longitudinal Data Systems*, Ch. 2 LDS Basics, https://nces.ed.gov/forum/ldsguide/book1/ch_2_1.asp (last visited Feb. 28, 2023).

[17] The Student Privacy Compass, *supra* note 13.

[18] *Id.*

[19] *Id.; see also* LearnPlatform, *supra* note 12 (discussing Minnesota, Illinois, and New York student data privacy legislation).

[20] LearnPlatform, *supra* note 12.

[21] 20 U.S.C. s. 1232g; 34 C.F.R. pt. 99.

[22] 20 U.S.C. s. 1232h; 34 C.F.R. pt. 98.

[23] 15 U.S.C. ss. 6501-06; 16 C.F.R. pt. 312.

Family Educational Rights and Privacy Act (FERPA)

FERPA protects the privacy of students' education records.[24] The law applies to any school that receives applicable funds from the U.S. Department of Education. FERPA grants parents certain rights respecting their child's education records, and this privacy right transfers to the student when he or she reaches age 18 or attends a post-secondary school (at which point he or she is known as an "eligible student").[25]

Parents or eligible students have the right to inspect and review the student's education records maintained by the school. They also have the right to request that a school correct records that they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.[26]

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions:

- School officials having a legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- Persons authorized to receive the records pursuant to a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific state law.[27]

Schools may disclose, without consent, directory information, such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must allow parents and students to opt out of the disclosure of their directory information. Schools must give an annual notice about rights granted by FERPA to affected parties.[28]

[24] U.S. Department of Education, *Family Educational Rights and Privacy Act (FERPA)* (Aug. 25, 2021), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*

Protection of Pupil Rights Amendment (PPRA)

PPRA applies to programs and activities that get their funding from the U.S. Department of Education.[29] It governs the administration to students of a survey, analysis, or evaluation that concerns one or more of the following eight protected areas:

- Political affiliations or beliefs of the student or the student's parent;
- Mental or psychological problems of the student or the student's family;
- Sex behavior or attitudes;
- Illegal, anti-social, self-incriminating, or demeaning behavior;
- Critical appraisals of other individuals with whom respondents have close family relationships;
- Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
- Religious practices, affiliations, or beliefs of the student or student's parent; or
- Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).[30]

PPRA also concerns marketing surveys and other areas of student privacy, parental access to information, and the administration of certain physical examinations to minors. The rights under PPRA transfer from the parents to a student who is 18 years old or an emancipated minor under state law.[31]

Children's Online Privacy Protection Act (COPPA)

COPPA and its related rules regulate websites' collection and use of children's information.[32] The operator of a website or online service that is directed to children, or that has actual knowledge that it collects children's personal information (covered entities), must comply with requirements regarding data collection and use, privacy policy notifications, and data security. For purposes of COPPA, children are individuals under the age of 13.[33]

COPPA defines personal information as individually identifiable information about an individual that is collected online, including:

- First and last name;
- A home or other physical address including street name and name of a city or town;
- Online contact information;
- A screen or user name that functions as online contact information;
- A telephone number;
- A social security number;
- A persistent identifier that can be used to recognize a user over time and across different websites or online services;

---

[29] U.S. Department of Education, *What is the Protection of Pupil Rights Amendment (PPRA)?*, https://studentprivacy.ed.gov/faq/what-protection-pupil-rights-amendment-ppra (last visited Feb. 27, 2023).
[30] *Id.*
[31] *Id.*
[32] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions*, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Feb. 27, 2023).
[33] *Id.*

- A photograph, video, or audio file, where such file contains a child's image or voice;
- Geolocation information sufficient to identify street name and name of a city or town; or
- Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above.[34]

Operators covered by the rule must:

- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;
- Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children;
- Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);
- Provide parents access to their child's personal information to review or have the information deleted;
- Give parents the opportunity to prevent further use or online collection of a child's personal information;
- Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security;
- Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use; and
- Not condition a child's participation in an online activity on the child providing more information than is reasonably necessary to participate in that activity.[35]

Violations of COPPA are deemed an unfair or deceptive act or practice and are therefore prosecuted by the Federal Trade Commission.[36]

Required Instruction in Florida Schools

The mission of Florida's K-20 education system is to allow its students to increase their proficiency by allowing them the opportunity to expand their knowledge and skills through rigorous and relevant learning opportunities.[37] Each district school board must provide appropriate instruction to ensure that students meet State Board of Education (SBE) adopted standards in the following subject areas: reading and other language arts, mathematics, science, social studies, foreign languages, health and physical education, and the arts.[38] Subject to the

[34] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions*, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Feb. 27, 2023).
[35] *Id.*
[36] *See id.; see also* 15 U.S.C. s. 6502(c); 16 C.F.R. s. 312.9.
[37] Section 1000.03(4), F.S.
[38] Section 1003.42(1), F.S.

rules of the SBE and the district school board, public school instructional staff[39] must also provide instruction in several other subject matters.[40]

III. Effect of Proposed Changes:

SB 662 creates s. 1006.1494, F.S., entitled "Student online personal information protection." The section generally limits and regulates the collection and use of K-12 student data by operators of Internet websites, online services, online applications, and mobile applications for K-12 school purposes. Among other things, the section prohibits operators from engaging in targeted advertising; places new and significant restrictions on operators' collection and use of K-12 students' data; prohibits operators from sharing, selling, or renting such data; and requires operators to adhere to new baseline privacy and security protections in connection with such data.

Definitions

The bill defines "covered information" to mean the personal identifying information or material of a student, or information linked to personal identifying information or material of a student, in any media or format that is not publicly available and is any of the following:

- Created by or provided to an operator by the student, or the student's parent or legal guardian, in the course of the student's, parent's, or legal guardian's use of the operator's site, service, or application for K-12 school purposes.
- Created by or provided to an operator by an employee or agent of a K-12 school or school district for K-12 school purposes.
- Gathered by an operator through the operation of its site, service, or application for K-12 school purposes and personally identifies a student, including, but not limited to, information in the student's educational record or electronic mail, first and last name, home address, telephone number, electronic mail address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

The bill defines "interactive computer service" to mean any information, service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

The bill incorporates by reference the existing definition for "K-12 school" in state law.[41] K-12 schools include charter schools and consist of kindergarten classes; elementary, middle, and high school grades and special classes; virtual instruction programs; workforce education; career centers; adult, part-time, and evening schools, courses, or classes, as authorized by law to be

[39] Instructional staff of charter schools are generally exempt from this section of law. Section 1002.33(16), F.S.
[40] Section 1003.42(2)(a)-(t), F.S. (listing a number of subject matters including, among others, the history of the U.S., the state, African Americans, and the Holocaust).
[41] Section 1000.04(2), F.S.

operated under the control of district school boards; and lab schools operated under the control of state universities.

The bill defines "K-12 school purposes" to mean purposes directed by or that customarily take place at the direction of a K-12 school, teacher, or school district or that aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or that are otherwise for the use and benefit of the school.

The bill defines "operator" to mean – to the extent that it is operating in this capacity – the operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or online application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes.

The bill incorporates by reference the existing definition for "school district" in state law.[42] "School district" means any of the 67 county school districts, including their respective district school boards.

The bill defines "targeted advertising" to mean presenting advertisements to a student which are selected on the basis of information obtained or inferred over time from that student's online behavior, usage of applications, or covered information. The term does not include advertising to a student at an online location based upon the student's current visit to that location, or advertising presented in response to a student's request for information or feedback, if the student's online activities or requests are not retained over time for the purpose of targeting subsequent advertisements to that student.

Prohibitions

The bill prohibits operators from knowingly:

- Engaging in targeted advertising on the operator's site, service, or application, or targeted advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, which the operator has acquired because of the use of that operator's site, service, or application for K-12 purposes.
- Using information, including persistent unique identifiers, created or gathered by the operator's site, service, or application to amass a profile of a student, except in furtherance of K-12 school purposes. The term "amass a profile" does not include the collection and retention of account information that remains under the control of the student or the student's parent or guardian or K-12 school.
- Sharing, selling, or renting a student's information, including covered information. This paragraph does not apply to the purchase, merger, or other acquisition of an operator by another entity, if the operator or successor entity complies with this section regarding previously acquired student information, or to a national assessment provider if the provider obtains the express written consent of the parent or student, given in response to clear and

[42] Section 595.402(5), F.S.

conspicuous notice, solely to provide access to employment, educational scholarships or financial aid, or postsecondary educational opportunities.

- Disclosing covered information, except as otherwise provided in the bill, unless the disclosure is made for any of the following reasons:
  - In furtherance of the K-12 school purpose of the site, service, or application, if the recipient of the covered information that is disclosed does not further disclose the information, unless such disclosure is made to allow or improve operability and functionality of the operator's site, service, or application.
  - To ensure legal and regulatory compliance or protect against liability.
  - To respond to or participate in the judicial process.
  - To protect the safety or integrity of users of the site or others or the security of the site, service, or application.
  - For a school, educational, or employment purpose requested by the student or the student's parent or guardian, provided that the information is not used or further disclosed for any other purpose.
  - To a third party, if the operator contractually prohibits the third party from using any covered information for any purpose other than providing the contracted service to or on behalf of the operator, prohibits the third party from disclosing any covered information provided by the operator with subsequent third parties, and requires the third party to implement and maintain reasonable security procedures and practices.

Requirements

The bill requires operators to:

- Collect no more covered information than is reasonably necessary to operate an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 purposes.
- Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information which are designed to protect it from unauthorized access, destruction, use, modification, or disclosure.
- Within a reasonable timeframe, delete a student's covered information if the K-12 school or school district requests deletion of covered information under the control of the K-12 school or school district, unless a student or a parent or guardian consents to the maintenance of the covered information.

Permitted Disclosures

The bill provides that an operator may use or disclose covered information of a student if:

- Federal or state law requires the operator to disclose the information, and the operator complies with federal or state law, as applicable, in protecting and disclosing that information.
- It is disclosed for legitimate research purposes, as required by state or federal law and subject to restrictions imposed thereunder, if covered information is not used for advertising or to amass a profile of the student for purposes other than K-12 school purposes; or as allowed by state or federal law and in furtherance of K-12 school purposes or postsecondary education purposes.

- The covered information is disclosed to a state or local educational agency, including K-12 schools and school districts, for K-12 school purposes, as allowed under state or federal law.

Permitted Activities

The bill provides that its terms do not prohibit an operator from:

- Using covered information to improve educational products, if that information is not associated with an identified student within the operator's site, service, or application, or other sites, services, or applications owned by the operator.
- Using covered information that is not associated with an identified student to demonstrate the effectiveness of the operator's products or services, including use in their marketing.
- Sharing covered information that is not associated with an identified student for the development and improvement of educational sites, services, or applications.
- Using recommendation engines to recommend to a student any of the following:
    - Additional content relating to an education, an employment, or any other learning opportunity purpose within an online site, service, or application, if the recommendation is not determined in whole or in part by payment or other consideration from a third party.
    - Additional services relating to an educational, an employment, or any other learning opportunity purpose within an online site, service, or application, if the recommendation is not determined in whole or in part by payment or other consideration from a third party.
- Responding to a student's request for information or feedback without the information or response being determined in whole or in part by payment or other consideration from a third party.

Unregulated Activities

The bill provides that it does not:

- Limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or under a court order.
- Limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes.
- Apply to general audience Internet websites, general audience online services, general audience online applications, or general audience mobile applications, even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications.
- Limit service providers from providing Internet connectivity to schools or students and their families.
- Prohibit an operator of an Internet website, online service, online application, or mobile application from marketing educational products directly to parents, if such marketing did not result from the use of covered information obtained by the operator through the provision of services covered under the bill.
- Impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this bill on such software or applications.

- Impose a duty upon a provider of an interactive computer service to review or enforce compliance with this bill by third-party content providers.
- Prohibit students from downloading, exporting, transferring, saving, or maintaining their own student data or documents.

Effective Date

The bill takes effect on July 1, 2023.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Because the bill prohibits operators from engaging in targeted advertising; places new and significant restrictions on operators' collection and use of students' online personal information; and prohibits operators from sharing, selling, or renting such information, operators will no longer be able to financially benefit from such activities. Additionally, because the bill requires operators to adhere to new baseline privacy and security protections in connection with students' online personal information, operators will incur costs associated with implementing these measures and complying with the bill.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill creates section 1006.1494 of the Florida Statutes.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.