HOUSE OF REPRESENTATIVES STAFF FINAL BILL ANALYSIS

BILL #: CS/HB 699 Student Online Personal Information Protection
SPONSOR(S): Education & Employment Committee, Koster and others
TIED BILLS: None. **IDEN./SIM. BILLS:** SB 662

FINAL HOUSE FLOOR ACTION: 118 **Y's** 0 **N's** **GOVERNOR'S ACTION:** Approved

SUMMARY ANALYSIS

CS/HB 699 passed the House on May 2, 2023, as SB 662 as amended. The Senate concurred in the House amendment to the Senate bill and subsequently passed the bill as amended on May 3, 2023.

To protect the private information of Florida's students, especially given the increased reliance on online platforms in schools, the bill creates the Student Online Personal Information Protection Act (SOPIPA), 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 using any information acquired through the use of their education technology to create profiles of students, except for K-12 school purposes, or knowingly engaging in targeted advertising. Additionally, the bill prohibits an operator from sharing, selling, or renting student information to third parties or disclosing certain covered information, except when authorized by federal or state law.

The bill requires operators to collect no more covered information than reasonably necessary to operate the educational technology and implement and maintain reasonable security procedures and practices to protect covered information. Operators must 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.

Any violation of the SOPIPA is deemed a deceptive and unfair trade practice and constitutes a violation of Florida's Deceptive and Unfair Trade Practices Act. However, there is no private cause of action for violations of SOPIPA, only the Department of Legal Affairs has enforcement authority.

The bill does not appear to have a fiscal impact to state or local governments. The bill has an indeterminate fiscal impact on the private sector.

The bill was approved by the Governor on May 31, 2023, ch. 2023-170, L.O.F., and will become effective on July 1, 2023.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF CHANGES:

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 of 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 information on race, location, gender, age, school, and 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 activity 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 collect 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 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

---

[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) (last visited May 4, 2023).

[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 (last visited May 4, 2023).

[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/ (last visited May 4, 2023).

[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 May 4, 2023).

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]

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:[11] the Family Educational Rights and Privacy Act (FERPA),[12] the Protection of Pupil Rights Amendment (PPRA),[13] and the Children's Online Privacy Protection Act (COPPA).[14]

Family Educational Rights and Privacy Act

FERPA protects the privacy of students' education records.[15] 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 these rights transfer to the student when he or she reaches the age of 18 or attends a post-secondary school (at which point he or she is known as an "eligible student").[16]

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.[17]

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

---

[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/ (last visited May 4, 2023).

[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) (last visited May 4, 2023).

[11] LearnPlatform, *supra* note 2.

[12] 20 U.S.C. s. 1232g; 34 C.F.R. pt. 99.

[13] 20 U.S.C. s. 1232h; 34 C.F.R. pt. 98.

[14] 15 U.S.C. ss. 6501-06; 16 C.F.R. pt. 312.

[15] 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.

[16] *Id.*

[17] *Id.*

- State and local authorities, within a juvenile justice system, pursuant to specific state law.[18]

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.[19]

Protection of Pupil Rights Amendment

The Protection of Pupil Rights Amendment (PPRA) applies to programs and activities that get their funding from the U.S. Department of Education.[20] 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).[21]

PPRA also governs 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.[22]

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) and its related rules regulate websites' collection and use of children's information.[23] 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.[24]

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;

---

[18] *Id.*
[19] *Id.*
[20] 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 May 4, 2023).
[21] *Id.*
[22] *Id.*
[23] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions,* https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited May 4, 2023).
[24] *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.[25]

Covered entities 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;
- Allow parents to consent 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;
- Allow parents 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.[26]

Violations of COPPA are deemed an unfair or deceptive act or practice and are therefore prosecuted by the Federal Trade Commission.[27]

State Student Privacy Legislation

At the state level, 42 states and the District of Columbia have passed more than 128 student privacy laws.[28] Indeed, most states have passed more than one student privacy law.[29]

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.[30]

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

---

[25] *Id.*
[26] *Id.*
[27] *See id.; see also* 15 U.S.C. s. 6502(c) and 16 C.F.R. s. 312.9.
[28] 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) (citing a senior technologist with at the Future of Privacy Forum at https://fpf.org/) (last visited May 4, 2023).
[29] 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 May 4, 2023); *see also* Student Privacy Compass, *State Student Privacy Laws*, https://studentprivacycompass.org/state-laws/ (last visited May 4, 2023) (maintaining a running list of state student privacy laws).
[30] The Student Privacy Compass, *Policymakers: Student [State] Laws and Legislation*, https://studentprivacycompass.org/audiences/policymakers/ (last visited May 4, 2023).

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.[31]

An example of the second approach is California's Student Online Personal Information Protection Act (CSOPIPA), which prevents online service providers from using student data for commercial purposes, while allowing specific beneficial uses such as personalized learning. California supplemented CSOPIPA 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 CSOPIPA 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.[32]

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

- To regulate its state longitudinal data system,[33] 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 CSOPIPA-like regulation of third parties, this approach has allowed innovative uses of student data while establishing meaningful privacy protections for students.[34]
- 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.[35]

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.[36]

Protections for Student Records and Data in Florida

Since the adoption of FERPA, Florida has aligned its protections for student educational records with the federal requirements.[37] Additionally, Florida law requires that the State Board of Education (SBE) adopt rules to implement protections for education records.[38]

In 2009, the Legislature adopted a public records exemption for student education records to provide additional protections for these records.[39] The law also clarifies that governmental entities that receive

---

[31] *Id.*; *see also* State of Oklahoma, Department of Education, *Data Privacy and Security*, https://sde.ok.gov/data-privacy-and-security (last visited May 4, 2023) (describing, among other things, certain important provisions of the Student DATA Act of 2013).
[32] The Student Privacy Compass, *supra* note 30; *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, CSOPIPA's provisions).
[33] 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 May 4, 2023).
[34] The Student Privacy Compass, *supra* note 29.
[35] *Id.*
[36] *Id.*; *see also* LearnPlatform, *supra* note 2 (discussing Minnesota, Illinois, and New York student data privacy legislation).
[37] Section 1002.22, F.S.
[38] Section 1002.22(3)(a), F.S. *See* r. 6A-1.0955, F.A.C.
[39] Section 1002.221(1), F.S.

education records from school districts or the DOE must maintain the confidentiality of these records in accordance with FERPA and the public records exemption.[40]

In 2014, the Legislature adopted additional protections for student data by prohibiting the collection of information on political affiliation, voting history, religious affiliation, or biometric information of a student or a parent or sibling of the student.[41] This provision also provided guidance on when educational records may be released to specified entities.[42] Finally, the Legislature placed additional restrictions on the identification and use of information designated as "directory information" under FERPA.[43] Specifically, the designation of directory information must occur at a regularly scheduled meeting of the governing board of an agency or institutions holding education records and the governing board must consider whether designation of such information would put students at risk of becoming targets of marketing campaigns, the media, or criminal acts.[44]

In 2021, the Parents' Bill of Rights was adopted by the Legislature and it required written consent by a parent prior to any of the following:

- a biometric scan of his or her minor child being made, shared, or stored;
- any record of his or her minor child's blood or deoxyribonucleic acid (DNA) being created, stored, or shared; and
- the state or any of its political subdivisions making a video or voice recording of his or her minor child.[45]

The Florida Deceptive and Unfair Trade Practices Act

The Florida Deceptive and Unfair Trade Practices Act (FDUTPA) is a consumer and business protection measure that prohibits unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in trade or commerce.[46] The FDUTPA is based on federal law.[47]

For example, Florida has determined that the following acts or practices are unfair or deceptive:

- Imposing unconscionable prices for the rental or lease of any dwelling unit or self-storage facility during a period of declared state of emergency;[48]
- Failing to abide by storage requirements for personal information and notice requirements for data breaches of such information;[49] and
- Failing to abide by requirements for weight-loss programs.[50]

The state attorney or the Department of Legal Affairs (DLA) may bring FDUTPA actions, if it serves the public interest, on behalf of consumers or governmental entities.[51] The Office of the State Attorney

---

[40] Section 1002.221(2)(b), F.S.
[41] Section 1002.222(1)(a), F.S.
[42] Section 1002.222(1)(b), F.S.
[43] Section 1002.222(2), F.S.
[44] *Id*.
[45] Section 1014.04(1), F.S. However, such information may be released without prior written consent as authorized by law. *Id*.
[46] Chapter 73-124, L.O.F., and s. 501.202, F.S.
[47] D. Matthew Allen, et. al., *The Federal Character of Florida's Deceptive and Unfair Trade Practices Act*, 65 U. MIAMI L. REV. 1083 (Summer 2011).
[48] Section 501.160, F.S.
[49] Section 501.171, F.S.
[50] Section 501.0579, F.S.
[51] Section 501.207(1)(c) and (2), F.S.; *see* s. 501.203(2), F.S. (defining "enforcing authority" and referring to the office of the state attorney if a violation occurs in or affects the judicial circuit under the office's jurisdiction; or the Department of Legal Affairs if the violation occurs in more than one circuit; or if the office of the state attorney defers to the department in writing; or fails to act within a specified period.); *see also* David J. Federbush, *FDUTPA for Civil Antitrust: Additional Conduct, Party, and Geographic Coverage; State Actions for Consumer Restitution*, 76 FLORIDA BAR JOURNAL 52, Dec. 2002 (analyzing the merits of FDUPTA and the potential for deterrence of anticompetitive conduct in Florida), http://www.floridabar.org/divcom/jn/jnjournal01.nsf/c0d731e03de9828d852574580042ae7a/99aa165b7d8ac8a485256c8300791ec1!OpenDocument&Highlight=0,business,Division* (last visited on May 4, 2023).

(SAO) may enforce FDUTPA violations occurring in its jurisdiction. DLA has enforcement authority if the violation is multi-jurisdictional, the state attorney defers in writing, or the state attorney fails to act within 90 days after a written complaint is filed.[52] Consumers may also file suit through private actions.[53]

DLA and the SAO have powers to investigate FDUTPA claims, which include:[54]

- Administering oaths and affirmations;
- Subpoenaing witnesses or matter; and
- Collecting evidence.

DLA and the SAO, as enforcing authorities, may seek the following remedies:

- Declaratory judgments;
- Injunctive relief;
- Actual damages on behalf of consumers and businesses;
- Cease and desist orders; and
- Civil penalties of up to $10,000 per willful violation.[55]

Effect of the Bill

The bill creates the "Student Online Personal Information Protection Act" (SOPIPA). The bill 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 bill 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.

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.

---

[52] Section 501.203(2), F.S.
[53] Section 501.211, F.S.
[54] Section 501.206(1), F.S.
[55] Sections 501.207(1), 501.208, and 501.2075, F.S. Civil Penalties are deposited into the General Revenue fund. Enforcing authorities may also request attorney fees and costs of investigation or litigation. Section 501.2105, F.S.

The bill incorporates by reference the existing definition for "K-12 school" in state law.[56] 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 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, or the site, service, or application was designed and marketed for K-12 school purposes.

The bill incorporates by reference the existing definition for "school district" in state law.[57] "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.

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 which the operator has acquired because of the use of that operator's site, service, or application for K-12 purposes.
- Using covered information 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. This prohibition does not apply to the purchase, merger, or other acquisition of an operator by third party, if the third party complies with the SOPIPA 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 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 disclosed does not further disclose the information.
    - Disclosure is required by state or federal law.
    - To comply with the order of a court or quasi-judicial entity.
    - To protect the safety or integrity of users of the site or others or the security of the site, service, or application.

[56] Section 1000.04(2), F.S.
[57] Section 595.402(5), F.S.

    - 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.

The bill requires that operators with actual knowledge that the site, service, or application is used primarily for K-12 school purposes or the site, service, or application was designed and marketed for K-12 purposes collect no more covered information than is reasonably necessary to operate an Internet website, online service, online application, or mobile application. Additionally, operators must 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. Finally, unless a parent or guardian expressly consents, in writing, to retaining student's covered information, the operator must delete the covered information at the conclusion of the course or corresponding program and no later than 90 days after a student is no longer enrolled in a school within the district, upon notice by the school district.

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. Additionally, the bill permits disclosure to a state or local educational agency, including K-12 schools and school districts, for K-12 school purposes. All such disclosures must comply with all requirements of federal and state law, as applicable.

The bill does 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.

Additionally, 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.
- Limit the retention of covered information by an operator for the purposes of assessments and college and career planning in accordance with general law.

The bill provides that any violation of the SOPIPA is a deceptive and unfair trade practice and constitutes a violation of the FDUTPA. However, there is no private cause of action for violations of SOPIPA, only the Department of Legal Affairs has enforcement authority.

The bill authorizes the SBE to adopt rules in implement the SOPIPA.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   None.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

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.

D. FISCAL COMMENTS:

None.