FPF Guide to Protecting Student Data Under SOPIPA:

For K-12 School Administrators and Ed Tech Vendors

November 2016

FPF Guide to Student Data Protection Under SOPIPA:
For K-12 School Administrators and Ed Tech Vendors[1]

[1] Authored by Brenda Leong, Future of Privacy Forum; Linnette Attai, PlayWell LLC; Amelia Vance, National Association of State Boards of Education; and David Rubin, David B. Rubin, PC

FPF Guide to Student Data Protections Under SOPIPA:
For K-12 School Administrators and Ed Tech Vendors

Introduction

This guide is designed to provide an overview of the California Student Online Personal Information Protection Act ("SOPIPA"), which – in conjunction with California Education Code section 49073.1 (formerly AB 1584) – was the first state law to comprehensively address student privacy. It became effective January 1, 2016 and applies to websites, applications, and online services that provide programs or services for K-12 students. SOPIPA applies to operators (as defined in the statute) that collect covered information from students in the state of California. This guide provides general information, not legal advice, and following the recommendations or tips within does not guarantee compliance with any particular law.

SOPIPA is important because most education technology companies do business with California schools, and because it became a template for similar statutes around the country. Our goal is to clearly explain what companies and information is covered, and what the law does (or doesn't) require. This may be useful for companies and schools operating in California now, and also may prove helpful to policymakers in those states who may still be considering updates to their student privacy laws, and are considering whether to follow the California model. Our discussion expands on:

- **Who must comply**? SOPIPA applies to operators of websites, online services (including cloud computing services), online applications or mobile applications *with actual knowledge* that their site, service or application is used primarily for *K-12 school purposes* and was designed and marketed for K-12 school purposes. SOPIPA does not apply to operators of general audience products, even if those products are accessible through a K-12 operator's product.

- **What is actual knowledge?** SOPIPA is silent on the question. The existing Federal Trade Commission (FTC) standard is a reasonable guide: The actual knowledge standard is likely to be met when an operator either communicates the nature of its content to a third party or when a representative of the third party recognizes the nature of the content. Ultimately, the FTC emphasizes a case-by-case approach.

- **What are K-12 school purposes?** Purposes that customarily take place at the direction of a K–12 school, teacher, or school district – *those direct activities traditionally and routinely done by the school as part of carrying out the education of its students*. Further, K-12 purposes may include secondary activities which aid of the administration of school activities, including in the classroom or at home, by school administration, between students, school personnel, or parents, or otherwise for the use and benefit of the school.

- **What is covered information?** Covered information is defined as personally identifiable information or materials, regardless of media or format, which meet any of several specified criteria. Most covered information is already identified and protected under FERPA.

- **What is unique to SOPIPA for Ed Tech vendors?**

Operators must not:

- Engage in targeted advertising when the targeting is based on any information that has been acquired because of the use of that operator's site, service or application
- Use information to amass a profile about a K-12 student, except in furtherance of a K-12 school purpose
- Sell a student's information, including covered information
- Disclose covered information except in specific, limited circumstances

Operators must:

- Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information
- Protect covered information from unauthorized access, destruction, use, modification, or disclosure
- Delete a student's covered information if requested by the school or district that controls the information[2]

- **What is Targeted Advertising?** A complicated question that is covered in detail below.

- **When can an operator disclose covered information?** To further the K-12 purpose of the site, service or application, provided that the recipient is likewise restricted; for legal response and compliance; for user safety; to other educational agencies for K-12 school purposes; and to other service providers when they are likewise contractually bound.

- **How else can operators use student information?** Operators may use student data to conduct legitimate research, and may use deidentified information for product improvement, marketing and development, or may use aggregated, deidentified information to develop and improve educational sites, services or applications.

---

[2] The "school official" exception under the Family Educational Rights and Protections Act (FERPA) already requires that operators be under the "direct control" of the educational agency as a condition of receiving student data. http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=16796a773ac48f980cdfaed80b1fa94a&rgn=div5&view=text&node=34:1.1.1.1.33&idno=34

- **SOPIPA rights for students:** Under SOPIPA, students may download, export or otherwise save or maintain data or documents that they create.

In addition to a detailed overview of SOPIPA, this guide also provides a general overview of federal student privacy laws, and a comparison to the other major state-level student privacy law, the Student User Privacy in Education Rights Act ("SUPER" Act), that as with SOPIPA, became a model for many states nationwide. The SUPER Act has its roots in the Student Privacy Pledge that the Future of Privacy Forum and Software & Information Industry Association facilitated with the education technology industry. Companies that take the pledge make 12 commitments, such as: not selling student data; not building student profiles for their own purposes; and disclosing how they use student data. Sample language for a bill based on these commitments was drafted and included in a variety of forms by many states.

Student Data Privacy – Background and Overview

Data use is now essential to most, if not all, education functions, and is so integral to the workings of schools and districts that it would be impossible to decouple data from education. Indeed, when data is being used effectively it allows parents to track and promote their children's progress, helps teachers improve their instruction and cater more accurately to students' needs, and assists school and district leaders in making managerial decisions, allocating resources, and communicating with the public. Constructive use of educational data also increases transparency, holds schools accountable, and helps state and federal policymakers assess policies and strategies prior to the enactment of important changes.

However, with the benefits of data come potential concerns. Collection, storage, access, and use of data all have inherent risks. Safeguarding student privacy is a critical aspect of responsible education data collection and use.

Children and adolescents are inherently vulnerable, and schools have a duty to protect their students from risks. This includes the misuse of, unauthorized access to, or theft of school-retained information, whether it exists on paper or is stored on a computer drive, in a network, or is informally shared. Most people think that maintaining their privacy is important. Despite numerous articles bemoaning young people's lack of attention to privacy issues, today's children do care about privacy; studies have found that the attitudes of older and younger people about privacy are similar, and a 2012 Microsoft study found that "[p]rivacy and security rank as college students' #1 concern about online activity."[3] Despite routine sharing of personal information in the digital age, most people, regardless of age, want to control who may access their personal data.[4]

---

[3] http://www.teachprivacy.com/do-young-people-care-about-privacy/

[4] USC Annenberg, *Is Online Privacy Over?,* April 22, 2013: "When asked about the statement, 'No one should ever be allowed to have access to my personal data or web behavior,' 70 percent of Millennials agreed, compared with 77 percent of users 35 and older." (http://annenberg.usc.edu/News%20and%20Events/News/130422CDF_Millennials.aspx)

Parental Concerns

As a Common Sense Media poll revealed, 90 percent of adults care about the ways that students' personal data becomes accessible to non-educational interests after it is collected as a part of instruction.[5] For some, "[e]ven if government were to keep the information private, the very existence of a 'dossier' is immensely intimidating and inhibiting."[6]

Other parents and students simply want to keep information they feel is embarrassing — whether poor test scores or a minor disciplinary event — private. Whether legitimate fear or paranoia, parents want to make sure childhood misjudgments, such as a fight in middle school, will not harm their child's future ability to attend college or get a job.

Moreover, as the scope and amount of educational and non-educational information that schools collect increases, the risks increase, as should security designed to mitigate those risks. Indeed, as public schools become more than just academic institutions — providing, for example, medical and psychological treatment in 2,000 school-based health centers around the country — they are continually collecting more information that is highly sensitive.[7]

At the same time, as examples of large-scale security breaches at businesses and government agencies emphasize, it is impossible for a company or a school to promise that it can keep information completely safe. As privacy advocate Joel Reidenberg observed, "You have failures at institutions that are spending millions trying to protect the security of their data. Is there any reason to believe that school systems are going to be more successful?"[8]

Education leaders and state policymakers hear concerns from many stakeholders about the collection and use of student data. Apprehensions abound, from those who fear "behavior modification"[9] to those who worry that children are learning to accept intrusions into their privacy.[10] Some concerns are part of more broadly held beliefs about privacy in general or about the role of government and public education. Other concerns reflect a lack

---

[5] Common Sense Media, *National Poll Commissioned by Common Sense Media Reveals Deep Concern for How Students' Personal Information Is Collected, Used, and Shared*, January 22, 2014 (https://www.commonsensemedia.org/about-us/news/press-releases/national-poll-commissioned-by-common-sense-media-reveals-deep-concern).
[6] Pioneer Institute: Big Data, Common Core, and National Testing
[7] Pioneer Institute: Big Data, Common Core, and National Testing
[8] Reidenberg, NPR: What Parents Need To Know About Big Data And Student Privacy.
[9] Pioneer Institute: Big Data, Common Core, and National Testing
[10] Jay Stanley, "Newest School RFID Scheme is Reminder of Technology's Surveillance Potential" *www.aclu.org*. June 29, 2012.

of basic, accurate information about data collection and use. Many concerns, however, are valid and important, especially those about the extent of data collected and the security of the technology used in data collection and storage.

For example, separate from concerns over data breaches and identity theft, many parents are worried about the potential ramifications of collecting so much data about children. They fear that the people, companies and government entities that create and maintain databases may misuse information or handle it poorly.[11] In its 2015 *Big Data* report, the White House warned that "[o]nce information about citizens is compiled for a defined purpose, the temptation to use it for other purposes can be considerable … If unchecked, big data could be a tool that substantially expands government power over citizens."[12] As an example, the report points to the use of supposedly confidential census data that was used to identify Japanese Americans for internment during the World War II.[13]

Another reason parents are often concerned about data collection is that children and adolescents often make mistakes when they are young that, if exposed, may affect their opportunities later in life. If discipline records became publicly accessible, it could be much harder for students to move past their bad choices. Yet many states collect information about student disciplinary incidents, often in great detail, and tie those records to students' names. For example, Louisiana has 32 different codes for disciplinary actions, and Florida has wide-ranging categories for student code violations.[14] The worry is that if disciplinary information is not expunged from school records, it could be used to deny students access to jobs in the future. Conversely, if it were to be expunged, it may hinder those who might intervene to help students make more positive behavior choices.

Criminal records are also included in many educational files. As of 2009, at least 17 states included a code for incarceration as a cause of withdrawal. [15] As researchers from Fordham University have observed, the "collection of data pertaining to the criminal justice system can be especially damaging to a student. Many states provide that juvenile criminal records can be sealed and eventually expunged. However, the incidents will still remain part of the student's education file in the absence of a comparable data purge requirement."[16] The question of cost/benefit of retaining such data is complex and raises concerns on all sides of the argument.

Concerns About Third Parties

[11] NPR: What Parents Need To Know About Big Data And Student Privacy
[12] BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, 22
[13] BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, 22
[14] Fordham Report: Children's Educational Records and Privacy 2009
[15] Fordham Report: Children's Educational Records and Privacy 2009
[16] Fordham Report: Children's Educational Records and Privacy 2009

Finally, there are ever-increasing numbers of third party educational applications used in the classroom, for purposes ranging from marking attendance and monitoring class behavior to learning new math skills. Because these apps are able to collect and maintain more student information than would ever have been maintained without technology — and, concerns about holding data without clear deletion or use restrictions — parents are concerned about what data these app providers collect regarding their child, and if the data could be used inappropriately.

In many ways, parental worries about what schools or other governmental entities might do with their child's data are the same as their worries about what third parties might do with the data. Focus on third parties and their access to student data has intensified over the past decade, not only because of the use of third party apps, but also because most schools outsource the electronic storage of educational records to third parties: ninety-five percent of districts rely on cloud-based services for a diverse range of functions, including data storage ("hosting") related to student performance, support for classroom activities, student guidance, and even cafeteria payments and transportation planning.[17]

While it may seem that student and school data would be more secure if stored on a local computer without access to the internet, like the paper files of old were kept in the school's locked back office, such a computer is subject to theft and damage. Storing data this way would also remove many of the benefits technology has brought to education, such as ensuring that transient students' records follow them so they don't fall behind, or allowing parents to know how their child is doing in class long before their mid-year report card.

It is also impractical for districts to build their own internet-connected networks to store student data: most schools and districts simply do not have the financial resources, technical expertise, or staffing capacity to develop their own internal systems. If schools and districts did create such systems without having the resources to manage them, the likelihood that student data would be mismanaged or inappropriately accessed would also increase. In addition, such systems would have to keep up with state and federal laws, which would likely require constant monitoring by the school district's legal counsel to verify that the district was not violating a complicated web of privacy laws. Finally, because some aggregate and individualized data must be reported at the state level, a district-created system could be incompatible with the state-level system, requiring increased staff time and new technology to make the systems compatible.

Therefore, many schools and districts contract with for-profit and nonprofit partners to transform their data into actionable information. Service providers have the capacity and expertise to securely manage and analyze data and provide timely, useful information to parents, educators, school leaders, and policymakers who use it to advance student success. Among these third parties, "cloud" providers are designed to provide complex, sophisticated privacy and security controls. Centralized systems, such as statewide longitudinal data systems and systems managed by service providers in the cloud, ensure that data collection,

[17] Fordham Report: Privacy and Cloud Computing in Public School 2013

storage, and access meet a uniform set of protections that limit the risk of inappropriate access and use.

Key Developments – the Student Privacy Pledge

While most vendors acknowledge the vital importance of student data privacy, they also want to ensure that any additional protections put in place do not hinder technological innovation in the classroom that could help students succeed: a representative for the Software and Information Industry Association, which represents many education technology companies, observed that policymakers looking to pass new laws or policies should assure that these "new legislative requirements … provide local communities and school officials with sufficient flexibility so that government actions intended to create a privacy and security floor do not unintentionally create a digital learning ceiling."[18]

However, the computer and tech industries have recognized the public's concerns about data privacy and security. As data security expert Tom Galvin explained, businesses "used to worry about who had the fastest speed or the most power or the most memory. Now they have to worry about whether consumers are going to fundamentally trust them."[19] This concern has led them to take several important steps toward self-regulation.

In 2014, the Software and Information Industry Association and the Future of Privacy Forum introduced a legally binding student data privacy pledge.[20] Over 200 companies have signed the pledge since it launched, and President Obama discussed the pledge favorably in his speech on data privacy in January 2015, where he stated that his administration would not hesitate to call out companies who did not sign on to it.

But some privacy experts note that this pledge and other self-imposed company guidelines may not be sufficient to deter so-called "bad actors" — software providers who want to exploit children's information and who will take advantage of holes in current laws to do so. In order to fill this gap, states like California have created laws that directly regulate third parties. Yet it is important to remember that many of the concerns parents have about third parties and student data — including worries that companies will use student data to market to children — are already illegal under existing federal laws, and "bad actors" have not yet been named.

Legal Overview

The **Family Educational Rights and Privacy Act** of 1974 (FERPA) is the main federal law that protects the privacy of student information, and is the basis for most state educational privacy laws. In general, FERPA protects students' education records from

---

[18] http://www.siia.net/blog/index.php/2014/05/siia-student-privacy-policy-guidelines-at-california-testimony/

[19] Byers, Alex. "Privacy as a PR Push." POLITICO. September 26, 2014. http://www.politico.com.

[20] http://studentprivacypledge.org/.

disclosure to people outside the education system, but makes an exception for "directory information," which can be released without the consent of the parent or student age 18 or older ("eligible student")..

FERPA identifies four rights that parents, guardians, or students age 18 and older have in regard to the student's education record and directory information:

1. **Inspect.** Parents have the right to inspect and review their child's education records.

2. **Correct.** Parents have the right to request that the school correct or amend their child's education records when the records are inaccurate or misleading. If the school decides not to amend the records, then the student (or parent/guardian) has the right to a formal hearing.

3. **Release.** Schools must obtain the written permission of parents to release any information from their child's education records, with certain exceptions. Schools may release records to the following parties *without* consent:
   - School officials with 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;
   - Authorized parties in a court case, to comply with 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.

4. **Opt out.** Schools must give parents the opportunity to opt out of having their children's directory information published.[21]

In response to state requests for clarification, Department of Education regulatory guidance for FERPA was updated in 2008, and again in 2011. These updates allow schools to consider contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions as "school officials" under FERPA.[22] This means schools may disclose student information to these parties without parental consent. However, these parties may not disclose the information to anyone else, and may use the information only for the purposes for which the disclosure was made.[23] The 2011 update allows schools to include student identification numbers with directory information only if

[21] 34 CFR §99
[22] 34 CFR §99.31
[23] 34 CFR §99.33

the numbers cannot be used to gain access to education records.[24] Outsourcing information to those parties was already a common practice by schools at that time; the FERPA updates simply clarified that this was acceptable under the law.

Compliance and Enforcement

FERPA is a "spending clause" statute, meaning that schools, districts, and state agencies must follow its provisions to be eligible to receive federal funds. Therefore, as a practical matter, all states must adhere to the provisions in FERPA. The Family Policy Compliance Office (FPCO) investigates complaints by students and parents or guardians regarding school, district, agency, or vendor compliance with FERPA.

FPCO will usually work with the school, district, or state agency to help it come into compliance with the law before moving to withhold funds. If a third party vendor is found to have violated FERPA, it can be excluded from having access to student information for up to five years. However, no school or vendor has ever been punished for violating FERPA through withholding funds or excluding access to student information.

As part of the 2011 FERPA regulation changes, the U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) to help schools, districts, and education policymakers with data privacy concerns related to student-level longitudinal data systems. In addressing student privacy, according to PTAC guidance, "[s]chools and districts are encouraged to remember that FERPA represents a minimum set of requirements to follow."[25] PTAC provides information and training materials and can offer direct assistance when needed.

COPPA

Enforced by the Federal Trade Commission, the Children's Online Privacy Protection Act (COPPA) regulates how commercial entities may collect and use personal information from children under the age of thirteen. The law's primary purpose is to put parents in control of information collected from their young children online by requiring their prior consent for the collection and use of that information.

COPPA allows schools to consent on behalf of parents to information collection by third-party website or online service providers who collect and use student personal information solely for the benefit of the schools, but for no other commercial purposes. Additionally, even if the school consents for the parents, the operator must still "provide the school with all the required notices … and upon request from the school, must provide a description of the types of personal information collected; an opportunity to review the

[24] 34 CFR §99.3
[25] PTAC, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, 2014, p.5.

child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information."[26]

In addition, the school may want to make available the operators' direct notices regarding their information practices for interested parents.

PPRA

Schools must also consider their obligations under the Protection of Pupil Rights Amendment (PPRA) to have policies in place and to provide direct notice to parents regarding "rights of parents to opt their children out of participation in, activities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or selling that information (or otherwise providing the information to others for that purpose)."[27]

When schools administer surveys and conduct analyses or evaluations funded by the U.S. Department of Education, such as surveys that help students discover what careers they might explore, PPRA defines the rules they must follow. PPRA requires that "schools and contractors make instructional materials available for inspection by parents if those materials will be used in connection with [a U.S. Department of Education]-funded survey, analysis, or evaluation in which their children participate."[28] As specified by the U.S. Department of Education, schools must also obtain written consent from parents or guardians before minor students are allowed to participate in surveys that ask questions regarding the following:

- political affiliations;
- mental and psychological problems potentially embarrassing to the student and his/her family;
- sexual behavior and attitudes;
- illegal, anti-social, self-incriminating and 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 guardian]; or
- income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).[29]

---

[26] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools

[27] Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, March 2015

[28] (citation needed)

[29] (citation needed)

PPRA is also enforced by the FPCO. Parents can file complaints with FPCO, and schools could lose federal funding if they do not comply with PPRA notice procedures. However, as with FERPA, FPCO will work with schools to come into compliance; to date no school has ever lost funding for not complying with PPRA notice procedures.

State Laws Generally

Prior to student data privacy taking off as an issue in 2014, many states had preexisting privacy laws. Some states have privacy laws that are not specific to education but still affect educational data. For example, 10 state constitutions have recognized a right to privacy,[30] and many more have general privacy protections in place for their citizens. These laws affect students, teachers, schools, and districts. Many states have specific laws regarding the disposal of records that contain personal information.[31] Some states also require government entities to have a written privacy policy in place.[32] And some, such as California, require government agencies to have a specific person responsible for compliance with privacy law.[33]

States can give students additional privacy protections, and many have: at least 35 states have passed laws supplementing FERPA;[34] 45 make their data privacy policies publically available; 48 state education agencies have established governance bodies charged with managing the collection and use of data, including how that data will be kept secure and confidential; and 45 have established policies that determine what type of data is available to select stakeholders, such as teachers and principals, who will use it to improve instruction.

The number of laws directly regulating student privacy has dramatically increased in the past three years. Since 2014, 49 states have introduced nearly 400 student privacy bills, with at least 100 bills introduced each year. Thirty-five states have passed 73 laws since 2013. Generally, these laws either regulate educational agencies and institutions, such as schools, districts, and state education agencies, or regulate third parties.

Thirty-three states have introduced either a version of California's SOPIPA or a similar piece of legislation that regulates industry known as the SUPER ("student user privacy in education rights") Act, and 12 states have passed those bills into law.

---

[30] "Constitutions in ten states—Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington—expressly recognize a right to privacy." National Conference of State Legislatures, *Privacy Protections in State Constitutions*, December 11, 2013.
[31] "At least 30 states have enacted laws that require entities to destroy, dispose, or otherwise make personal information unreadable or undecipherable." National Conference of State Legislatures, *Data Disposal Laws*, December 26, 2013.
[32] Cf. Alaska Stat. § 45.48.530; Ariz. Rev. Stat. Ann. § 41-4152; Colo. Rev. Stat. § 6-1.713; N.J. Stat. 56:8-162
[33] Cal. Civ. Code § 1798.22: "Each agency shall designate an agency employee to be responsible for ensuring that the agency complies with all of the provisions of this chapter."
[34] Epic.org, *Student Privacy*

SOPIPA, SUPER, and other recent student privacy laws impose direct liability on ed tech operators. FERPA, which is enforced by the U.S. Department of Education is only directly enforceable against "educational institutions receiving federal funds" – which equates to most public schools. Even if a third party vendor practice causes the school to be in violation of FERPA, DOE may only hold the school liable. Any liability by the school service provider would simply be through its contract with the school. The entire purpose of states seeking to pass SOPIPA, SUPER, and other student privacy laws is to directly regulate private companies that are now so frequently working directly with students as part of the

SOPIPA

The Student Online Personal Information Protection Act (SB 1177, or SOPIPA) is a California student data privacy regulation signed into law on September 29, 2014, and in effect since January 1, 2016. It has been described by California State Senate President Pro tempore Darrell Steinberg (D-Sacramento) as a law that "fosters innovation and protects kids' privacy."[35]

It is written broadly, providing new and extensive data privacy protections for K-12 students in California and unprecedented advertising restrictions.

SOPIPA is complemented in California by the privacy of pupil records provision of the California Education Code 49073.1[36] (commonly referred to as AB 1584), which authorizes educational agencies to contract with third party technology providers for educational software or for storage and management of pupil records. The Code requires that contracts between vendors and school systems:

- State that pupil records are the property of and under the control of the local educational agency
- Specify what measures a technology provider will take to ensure the security and confidentiality of pupil records
- Explain how the technology provider and educational agency will together ensure compliance with the Family Educational Rights and Privacy Act (FERPA)
- Prohibit third parties from using any information in the pupil record for any purpose other than those required or permitted by the contract.
- Explain how the parent or eligible pupil may review and correct personally identifiable information in the pupil's records
- Explain how affected parents or eligible pupils will be notified in the event of unauthorized disclosure of the pupil's records
- Certify that the pupil's records will not be retained or available to the vendor upon completion of the term of the contract and how that will be enforced

[35]http://blogs.edweek.org/edweek/DigitalEducation/2014/09/_landmark_student-data-privacy.html

[36] http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=EDC&sectionNum=49073.1

- Prohibit use of personally identifiable information in pupil records to engage in targeted advertising
- Describe how pupils may retain possession and control of their pupil-generated content, if applicable
- Contracts that don't align with AB 1584 can be considered void.

Together, SOPIPA and AB1584 create a comprehensive suite of data privacy regulations for operators in California.

Who Must Comply?

SOPIPA applies to operators of websites, online services (including cloud computing services), online applications or mobile applications *with actual knowledge* that their site, service or application is used primarily for *K-12 school purposes* **and** was designed and marketed for K-12 school purposes.

SOPIPA **does not apply** to operators of general audience products, even if those products are accessible through a K-12 operator's product. For example, if an operator designs and markets an educational website for K-12 school purposes, and includes a link to a general audience social media or video platform on the website, it is likely that the educational website will need to comply with SOPIPA, but the general audience social media or video platform would be exempt.

An operator does not need to have a contract with a school or district in order to be subject to SOPIPA. Instead, the need to comply is determined by the use, design and marketing of the product.

What is "Actual Knowledge"?

It may seem obvious, but this question was a subject of much discussion prior to the Federal Trade Commission's (FTC) 2012 update of the Children's Online Privacy Protection Act (COPPA). The focus there was on how and when a third party would be deemed to have "actual knowledge" that it was operating on a child-directed site.

SOPIPA is silent on the question. However, the existing FTC standard seems to provide a reasonable guide.

The FTC noted that the actual knowledge standard was likely to be met when an operator either communicated the nature of its content to the third party or when a representative of the third party recognized the nature of the content.

The FTC further noted that, while other facts might also be sufficient to establish actual knowledge, such facts would need to be analyzed carefully on a case-by-case basis.[37]

[37]https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf

If you are told that your product is used primarily for K-12 school purposes or you otherwise identify that as being the case, you have likely met the "actual knowledge" standard.

What are "K-12 School Purposes"?

Under SOPIPA, K-12 School Purposes has several key meanings, each of which helps clarify the use cases covered by the restrictions. Overall, they are purposes that customarily take place at the direction of the K–12 school, teacher, or school district – meaning *those direct activities traditionally and routinely done by the school as part of carrying out the education of its students*.

Further, K-12 purposes may be secondary activities which aid of the administration of school activities, including in the classroom or at home, by school administration, between students, school personnel, or parents, or otherwise for the use and benefit of the school.

Similarly, the SUPER bills include consistent language in their definition of a "school service." In those laws, school service means a web site, mobile application, or online service that:

(a) is designed and marketed primarily for use in a K-12 school;
(b) is used at the direction of teachers or other employees of a K-12 school; and
(c) collects, maintains, or uses student personal information.

Within this definition, SUPER laws *expressly exclude* websites, mobile applications, or online services that are designed and marketed for general use, even if they are also marketed in a way that includes promotions to K-12 schools. This means that common market products – a word processing program, an administrative management tool, even some children's apps or games – that are not specifically designed for an educational purpose and marketed directly to schools are not covered by the limitations of the bill.

SOPIPA has the same exception, as does almost every student privacy law in the country, regardless of model origin. This is a frequently misunderstood exclusion, but simply means that these laws do not apply to the wide variety of tools available to the general public, even if they are also used by schools. A vendor selling tools or providing services designed for the general public isn't obligated to redesign them just because schools purchase the products or students happen to visit the websites.

The use of these general products is still covered by existing, separate federal and state laws, which make it clear that schools are restricted from requiring students to share data except for appropriate educational purposes. If a school purchases a general audience product and requires students to use it, it is still ultimately responsible for making sure that the tool complies with privacy regulations that apply to the school.

What Information Is Protected Under SOPIPA ("Covered Information")?

SOPIPA protects a wide range of student information, referred to as "covered information." It includes information provided by the student, and information provided about the student by school representatives, parents and legal guardians.

Covered information is defined as personally identifiable information or materials, regardless of media or format, which meet any of the following criteria:

- Created or provided by a student, or the student's parent or legal guardian, to an operator in the course of their use of the operator's site, service, or application for K-12 school purposes
- Created or provided by an employee or agent of the K-12 school, school district, local education agency, or county office of education, to an operator
- Gathered by an operator through the operation of a site, service or application and is descriptive of a student or otherwise identifies a student, including, but not limited to these 29 items:

Information in the student's educational record or email ~ First and last name ~ Home address ~ Telephone number ~ Email address ~ 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 ~ Geolocation information

Most data elements categorized as "covered information" under SOPIPA are already protected as personally identifiable information under federal laws. For example, within FERPA, personally identifiable information includes, but is not limited to name and address of the student and family members, personal identifiers or biometric records, indirect identifiers and the very broadly inclusive: "other information that, *alone or in combination, is linked or linkable to a specific student* that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty, or information requested by a person who the educational agency reasonably believes knows the identity of the student to whom the education record relates.[38]

COPPA characterizes personal information to include not only name, address, online identifiers, photos and videos that contain a child's likeness and audio files that contain a child's voice, but also geolocation "sufficient to identify a street name and name of a city or town," as well as persistent identifiers that can be used to recognize a user over time and across different Web sites or online services.[39]

---

[38] 34 CFR §99.3
[39] 16 CFR §312.2

Under SOPIPA, the term "covered information" is meant to include "personally identifiable information," but unlike in many laws, "personally identifiable information" is not defined in SOPIPA. This creates compliance challenges for operators, because each operator needs to assess the data provided by the student or by teachers and parents about the student, and determine if it could be construed as personally identifiable.

The lack of specificity in the list of items deemed to be covered information compounds the issue. For example, coarse geolocation, sufficient to identify country, state or city, is not usually considered to be personally identifiable or "descriptive" of a student unless combined with other identifiable information. Capturing coarse geolocation (such as state) may be useful for operators to inform students about state-specific scholarships, or to block ads from students and parents in the state.

However, given that SOPIPA is silent on the question of what is personally identifiable, and that it offers no distinction between coarse and fine geolocation, operators must each make a judgment about what would be considered compliant.

In addition, covered information includes information that is "descriptive or otherwise identifies a student." However, what is descriptive is not often "otherwise identifiable." A student may be described as 12 years old, with brown hair and brown eyes, but one would not characterize that as "identifiable" unless dealing with an exceptionally small population or combining those descriptors with other information.

Operators also must exercise their own judgment to determine which "documents" are and are not categorized as descriptive or identifiable. Although the law references "all media, regardless of format," documents in particular are called out separately with no explanation, and so should be carefully evaluated for possible relevance under this section.

Operators will need to use care and caution when working through the factors, assess their risk and make a reasonable determination about what data is actually covered. One of the pitfalls of SOPIPA is that – in the absence of official guidance – such determinations may vary wildly across industry, or by what requirements may be set in different school districts, making state-wide compliance challenging or potentially contradictory.

Specific Requirements of SOPIPA for Ed Tech Vendors

Under SOPIPA, operators may not:

- Engage in targeted advertising on their site, service or application, or target advertising on any other site, service or application when the targeting is based on any information, including covered information and persistent unique identifiers, that has been acquired because of the use of that operator's site, service or application

- Use information, including persistent unique identifiers, created or gathered by the operator's site, service or application, to amass a profile about a K-12 student, except in furtherance of K-12 school purpose
- Sell a student's information, including covered information
- Disclose covered information except in specific, limited circumstances

Operators must:

- Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information
- Protect covered information from unauthorized access, destruction, use, modification, or disclosure
- Delete a student's covered information if requested by the school or district that controls the information[40]

What is Targeted Advertising?

This is one of the most complex provisions of SOPIPA, primarily because it is not clearly defined. As a result, the prohibition creates a significant compliance challenge for operators, and leaves schools and operators with a lack of clarity about the role of ad supported technology in education. For more on the questions surrounding targeted advertising, see the Discussion Annex.

When Can an Operator Disclose Covered Information?

Covered information may be disclosed only to:

- Further the K-12 purpose of the site, service or application, provided that the recipient:
  - Does not then disclose the information unless to allow or improve operability and functionality within the student's classroom or school; *and*
  - Is legally required to implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information, and protect that information from unauthorized access, destruction, use, modification and disclosure
- Ensure legal and regulatory compliance
- Respond to or participate in judicial process
- Protect the safety of users or others, or the security of the site
- A state or local educational agency, including schools and school districts, for K-12 school purposes, as permitted by state or federal law

---

[40] The "school official" exception under the Family Educational Rights and Protections Act (FERPA) already requires that operators be under the "direct control" of the educational agency as a condition of receiving student data. http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=16796a773ac48f980cdfaed80b1fa94a&rgn=div5&view=text&node=34:1.1.1.1.33&idno=34

- A service provider, when the operator contractually:
    - Prohibits the service provider from using any covered information for any purpose other than providing the contracted service to, or on behalf of, the operator
    - Prohibits the service provider from disclosing any covered information provided by the operator with subsequent third parties
    - Requires the service provider to implement and maintain reasonable security procedures and practices as described above

How Can Operators Use Student Information?

Operators may use student data to conduct:

- Legitimate research, defined as:
    - Required by state or federal law and subject to the applicable legal restrictions
    - Allowed by state or federal law and under the direction of a school, school district or state department of education, *provided that covered information is not used for anything other than the K-12 school purposes*

Operators may use deidentified information for product improvement, marketing and development:

- Within any of their own sites, services or applications to improve educational products
- To demonstrate the effectiveness of the operator's products or services, including in their marketing.

Finally, operators may use aggregated, deidentified information to develop and improve educational sites, services or applications

SOPIPA Rights for Students

Under SOPIPA, students may download, export or otherwise save or maintain data or documents that they create. This is an important note for operators, as it allows for an independent relationship with the student user, who may wish to maintain continuity of their work over time. It is a provision that is not always being included in other state laws that are modeled after SOPIPA.

School and District Guidance on SOPIPA – What to Expect

While SOPIPA applies to technology providers, schools and districts want to ensure that operators comply with SOPIPA before engaging. A few districts in California have issued guidance to schools. However, the guidance is limited and varies widely.

Guidance available from the Los Angeles Unified School District,[41] which predates passage of SOPIPA, notes:

> "Indeed, a secondary market of application or 'App' development and educational product advertising has evolved around these online services that hold student personal information. Developers are using student data to design new applications that can be sold on these in-system K-12 online sites or 'stores.' 'Apps' purchased in these 'stores' often times have no privacy policy presented during the purchase. This is leaving student personal information vulnerable for a host of uses never contemplated by the students or educators. Current federal and state privacy laws are deficient in protecting student personal information. It is imperative that online companies that market their online sites to schools and students for K-12 school purposes ensure that the sensitive information they hold regarding California students remains safe."

When working with schools and districts in California, be prepared for questions, and a good deal of anxiety.

Several districts require that vendors answer checklists in the form of "yes/no" questions that list key provisions of both SOPIPA and AB 1584. Unfortunately, some of these checklists do not always track legal requirements, creating some concern.

When it comes to standardized or prescribed contract language, some schools or districts do not allow operators to correct mistakes in proposed contract terms, or to strike language that is not applicable to the product. As such, operators may be forced to find alternative ways to call out contractual provisions that are not relevant, or in extreme cases, may choose to not serve that district.

One district includes a standardized requirement that operators guarantee compliance with the entire California Education Code. Since the code deals with a wide variety of topics, including sex equity, violence prevention, county boards of education, election conduct, child care facilities, bonds, retirement and more that is not applicable to technology providers, this is something of a misfit for providers to assert, when it would be more appropriate to specify only the 49073.1 provisions, which are applicable.

Some schools and districts remain unfamiliar with the details, or sometimes even the broad outlines, of the new laws, and in those cases, the burden is particularly strong on the vendor to ensure that both sides are aware of the requirements, so they can work in partnership to fulfill them.

Some districts do not have privacy policies on their own websites or do not display them prominently, and are otherwise struggling with their own compliance practices. They are also frequently delaying development of their own SOPIPA-based requirements in the

[41] http://home.lausd.net/apps/search/?q=sopipa&x=0&y=0

expectation that the state will provide more detailed instruction. Until that happens, if it does, patience, knowledge, flexibility and guidance from the vendor will be invaluable to ease the fears, ensure compliance and help in crafting balanced and legally enforceable contracts.

Guidance from the State of California

Guidance emerging from the State Attorney General's office is in the form of "recommended practices." Since it is not being issued as binding regulatory interpretation to ensure compliance with SOPIPA, it does not carry the weight of law. While it provides a sensible approach to some areas of protecting student privacy, it does not further clarify some of the vaguer terms and requirements in SOPIPA. As such, operators will still bear the responsibility, in conjunction with guidance from counsel, to determine their thresholds for compliance. It may be that subsequent legal challenges are what end up defining the true scope of the law.

Legal Remedies

The enforcement authority and likelihood of action under SOPIPA are other aspects that diverge significantly from FERPA. Under FERPA, individuals do not have a private right of action – only DoEd may bring a claim against an educational institution for a violation. However, since the withholding of federal funds associated with a FERPA violation response could have extreme consequences for a school or district, FERPA budgetary withholding has never been implemented.

In contrast, SOPIPA provides a private right of action, in addition to actions which may be brought by the state Attorney General, so it is foreseeable that enforcement actions may occur more often and allow for more graduated penalties. Nevertheless, beyond establishing who may bring a claim by virtue of it being enforced under the California Business Code, SOPIPA contains no provisions for its own enforcement.

Currently, violations are expected to be addressed under California's far-reaching Unfair Competition Law ("the UCL"),[42] which defines "unfair competition" to include virtually any unlawful business practice.[43] The UCL authorizes enforcement proceedings by government officials such as the Attorney General, district attorneys, county counsel and city attorneys and, in more limited circumstances, by private individuals and entities.[44] A court may issue an injunction, requiring the wrongdoer to stop the violation. The court also may order restitution in the form of return of money or property lost as a result of the offending conduct,[45] or it may impose civil penalties. The UCL makes clear that its remedies

---

42 *See* California Business and Professions Code, §§ 17200 through 17209.

43 UCL, § 17200. *See also Comm. On Children's Television, Inc. v. Gen. Foods Corp.*, 35 Cal. 3d 197, 210 (1983).

44 UCL § 17204.

45 *See Madrid v. Perot Systems Corp.*, 130 *Cal.App.*4th 440, 452, 30 *Cal.Rptr.*3d 210 (2005).

are intended to supplement other existing law, so it is possible that victims may simultaneously seek relief under the UCL and other statutes that may offer protection based on the same facts.[46]

The UCL imposes significant limitations on the ability of private individuals and entities to sue under the statute. For many years, private parties were not required to show any actual injury or financial harm in order to bring a lawsuit under the UCL which, in the view of the business community and the Legislature, was "subject to abuse by attorneys who used it as the basis for legal '"shakedown'" schemes"[47] and frivolous lawsuits.[48] But a 2004 amendment to the UCL, known as Proposition 64, now requires private plaintiffs to show that they "suffered injury in fact and . . . lost money or property" as a result of the unfair competition. The phrase "injury in fact" is a technical legal term intended to permit only parties who have actually suffered demonstrable harm to bring suit, and to prevent lawsuits brought in the public interest by individuals or organizations who have not suffered harm themselves.

Showing "injury in fact and . . . lost money or property" could be a daunting challenge in cases involving improper disclosure of online personal data. Some data breach cases decided under the UCL, prior to SOPIPA, have allowed suits to go forward if plaintiffs could at least show that they paid more for an offending company's product than they would have had they known of the company's shoddy data security measures.[49] But unlawful dating mining, targeted advertising and other practices prohibited by SOPIPA may not involve payment of money by the aggrieved party, rendering even this low threshold of proof impossible to meet in many cases. This will be made ever more challenging by plaintiffs given the lack of specificity in key provisions of the law.

Since the same events triggering a violation of SOPIPA may also be sued upon if they violate other law, it can be anticipated that creative plaintiffs' counsel will attempt to develop viable theories of liability under the California Constitution's right of privacy clause,[50] and other state statutes. Since SOPIPA just became effective in January 2016, however, it is too soon to assess how receptive the California courts will be. Notwithstanding the viability of specific legal claims, since vendors who are the subject of

---

[46] UCL § 17205.

[47] See Buckland *v. Threshold Enterprises*, *Ltd.*, 155 *Cal.App.*4th 798, 812, 66 *Cal.Rptr.*3d 543 (2007), disapproved on other grounds in *Kwikset Corp. v. Superior Court*, 51 *Cal.*4th 310, 337, 120 *Cal.Rptr.*3d 741, 246 *P.*3d 877 (2011).

[48] See Californians *for Disability Rights v. Mervyn's LLC*, 39 *Cal.*4th 223, 228, 46 *Cal.Rptr.*3d 57, 138 *P.*3d 207 (2006).

[49] *In re Anthem, Inc. Data Breach Litigation,* ____ *F.Supp.*3d ____, 2016 WL 589760 (N.D. Cal. 2016); *In re Adobe Systems, Inc. Privacy Litigation*, No. 13-CV-05226-LHK, 2014 WL 4379916 (N.D. Cal. 2016) *16 (N.D. Cal. 2014). *See also In re Sony Gaming Networks & Customer Data Security Breach Litigation*, No. 11MD2258 AJB MDD, 2014 WL 223677 (S.D. Cal. 2014).

[50] Article I, section 1 of the *California Constitution* provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and *pursuing and obtaining* safety, happiness, and *privacy.*"

such actions are likely to experience reputational harm, they may want to consider a conservative approach and practice.

Which States Are Following California's Lead?

Seventeen states have passed laws that resemble or take inspiration from SOPIPA, resulting in 18 new laws:

Arkansas HB 1961 ~ California AB 2799 ~ Connecticut HB 5469 ~ Delaware SB 79 ~ Georgia SB 89 ~ Hawaii SB 2607 ~ Kansas SB 2008 ~ Maine LD 454 ~ Maryland HB 298 ~ Nevada SB 463 ~ New Hampshire HB 520 ~ North Carolina HB 632 ~ Oregon SB 187 ~ Tennessee HB 1931 ~ Virginia HB 1612 ~ Virginia HB 519 ~ Virginia HB 749 ~ Washington SB 5419

In all, 33 states have considered bills that resemble SOPIPA. Seven states have passed legislation with clauses modeled after SOPIPA in 2016,[51] a number that is likely outdated by the time you read this. Not every such bill or law includes all of the provisions of SOPIPA, and it remains to be seen how interpretation and enforcement of SOPIPA might influence legislative action across the country.

Key Differences:
Several state laws have more clearly defined preclusions around advertising, having clearly spent some time trying to carve out a more precise definition. For example, Virginia law clearly explains that operators may not, "use or share any student personal information for the purpose of behaviorally targeting advertisements to students,"[52] where "behaviorally targeting advertising" is a previously defined term for industry (see Annex, "What is Targeted Advertising?").

Oregon law precludes targeted advertising, but defines it as "advertising presented to a student based on information obtained or inferred from the student's online behavior, usage of applications or covered information." Targeted advertising under Oregon law does not include "advertising presented to a student at an online location based upon the student's current visit to that location or as a single search query, as long as the student's online activities are not collected or retained over time."[53]

Similarly, Georgia law defines targeted advertising as "presenting advertisements to a student where the advertisement is selected based on information obtained or inferred from that student's online behavior, usage of applications or student data," and that it does not include "advertising to a student at an online location based upon that student's current visit to that location or a single search query without collection and retention of a student's

[51] http://dataqualitycampaign.org/resource/2016-student-data-privacy-legislation/
[52] http://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+CHAP0728
[53] https://olis.leg.state.or.us/liz/2015R1/Downloads/MeasureDocument/SB187/Enrolled

online activities over time."[54] Still other states are looking at the student data privacy legislative landscape and, while enacting strong data privacy protections, are also taking steps to ensure that beneficial services are not unintentionally precluded by the laws. For example, Colorado law notes that its definition of targeted advertising specifically does not include use of a student's personally identifiable information to identify higher education institutions or scholarship providers that are looking for students who meet specific criteria, provided that it's done with the permission of the student or the student's parent.[55]

What Should Operators Do Now?

This resource should help you become familiar with the key requirements of SOPIPA, but it's just the beginning. As always when it comes to student data privacy, taking responsibility for proper and compliant stewardship of student data is a requirement for operating in the education arena, as is partnering in a positive and proactive manner with schools and districts.

In the absence of definitive state guidance, consult with competent legal counsel to assess any risk you might have with respect to SOPIPA, and ensure that your data privacy and security policies and practices are in alignment with all relevant and applicable federal, state and local laws and norms.

Reassess your third parties, their data handling practices and your contracts to be sure they contain the necessary restrictions. Also assess all current and future product development and data handling operations in accordance with the regulations, in partnership with competent legal and compliance guidance.

In addition, pay close attention to any authoritative regulatory guidance that emerges from California and other states.

Conclusion

This guide provides an overview of SOPIPA, comparing the California statute with federal law and other state statutes governing school service providers. As a reminder, nothing in this guide should be considered legal or compliance advice, and actions based on the interpretation and recommendations here cannot be guaranteed to ensure compliance with any particular law(s).

Clearly, guidance from the State of California would be helpful to interpret the vaguer points of SOPIPA. In its current form, it is unclear what specific actions will ensure operator

---

[54] https://legiscan.com/GA/text/SB89/2015

[55] http://www.leg.state.co.us/clics/clics2016a/csl.nsf/fsbillcont3/65C31D600337BF8787257F2400644D7C?open&file=1423_enr.pdf

compliance with some SOPIPA provisions; therefore, it is important for operators to remain aware of industry norms and to comply with the spirit of the regulation.

ANNEXES

A. Relevant Laws
B. What is Targeted Advertising?
C. What Can Parents Authorize?
D. What are “Reasonable Security” Procedures and Practices?[56]

[56] https://ferpasherpa.org/s-p.html#security

A. Relevant Laws

FEDERAL:

FERPA – Family Educational Rights and Privacy Act (20 U.S. Code § 1232g)

i. FERPA – Final Rule 2011 (34 CFR Part 99)
ii. FERPA – Department of Education Guidance for Eligible Students

COPPA – Children's On-Line Privacy and Protection Act (15 U.S. Code § 91)

i. FTC COPPA Rule, Guidance, and FAQs (16 CFR Part 312)

PPRA – Protection of Pupil Rights Amendment (20 U.S. Code § 1232h)

STATE

SOPIPA – Student Online Personal Information Protection Act (SB 1177)

CA Education Code/Privacy of Pupil Records– (49037.1))

Summary of Other State Laws – (Data Quality Campaign - 2016)

2015:
Arkansas HB 1961
Delaware SB 79
Georgia SB 89
Maine LD 454
Maryland HB 298
Nevada SB 463
New Hampshire HB 520
Oregon SB 187
Virginia HB 1612
Washington SB 5419

2016:
California AB 2799
Connecticut HB 5469
Hawaii SB 2607
Kansas SB 2008
North Carolina HB 632
Tennessee HB 1931
Virginia HB 519
Virginia HB 749

B. What is Targeted Advertising?

A critical provision of SOPIPA requires that operators do not, "Engage in targeted advertising on their site, service or application, or target advertising on any other site, service or application when the targeting is based on any information, including covered information and persistent unique identifiers, that have been acquired because of the use of that operator's site, service or application." The reference to "targeted advertising" has since been widely imitated in other state legislation, yet this provision is constructed so as to create both operational and possibly Constitutional issues that are worth discussion.

Before diving in further, it's important to review how the clause is actually written in the law. As constructed, it refers to two different types of advertising:

1. Targeted advertising on the operator's site, service or application; OR
2. Targeted advertising on any other site, service or application when the targeting is based on any information, including covered information and persistent unique identifiers, that have been acquired because of the use of that operator's site, service or application

To comply with the law, we first need to answer the question, "what is targeted advertising?" It's been the subject of much discussion and debate, as it is not defined in SOPIPA. Existing federal regulation, industry self-regulation and other guidance do not define it either. Instead, regulation most commonly uses the following terms.

Existing terms:

Behaviorally targeted advertising (also referred to as online behavioral advertising [OBA] or interest-based advertising) has been defined by the Digital Advertising Alliance[57] (DAA) as "the collection of data online from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate Web sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on preferences or interests known or inferred from the data collected."[58] Serving behaviorally targeted advertising does not actually require collection of personal information. Instead, a party will serve ads to a user based on a profile developed from tracking the computer browser activities over time and across different websites and online services.

[57] Digital Advertising Alliance is "an independent non-profit organization led by the leading advertising and marketing trade organizations." It represents a cross-industry self-regulatory program that "establishes and enforces responsible privacy practices across industry for relevant digital advertising, providing consumers with enhanced transparency and control." http://www.aboutads.info/

[58] http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf

The definition has largely been accepted by the FTC, and is described in similar fashion in its Self-Regulatory Principles for Online Behavioral Advertising.[59] This type of advertising is precluded by the Children's Online Privacy Protection Act (COPPA) for children under 13 without prior, verifiable parental consent, as well as by the existing self-regulatory advertising groups, including DAA and the Network Advertising Initiative (NAI).[60]

Contextual targeting (also referred to as contextually relevant advertising) is defined by DAA as advertisements that are delivered "based on the content of a Web page, a search query, or a user's contemporaneous behavior on the Web site."[61] NAI expands a bit further explaining, "the ad selected depends upon the content of the page on which it is served, or 'first party' marketing in which ads are customized or products are suggested based on the content of the page or users' activity on the page (including the content they view or the searches they perform)."[62]

The FTC echoes this in policy statements and in comments surrounding COPPA. There, the FTC notes that contextual targeting, "is more transparent and presents fewer privacy concerns as compared to the aggregation and use of data across sites and over time for marketing purposes." Contextual targeting is permitted under COPPA.

Why Does This Matter?

The definition of targeted advertising is critically important for a variety of reasons.

Consider the case of the student who progresses quickly through curriculum material and is ready for more. Perhaps the student is working on math lessons though a product used in school and at home. After completing the work assigned by the teacher, would the operator be able to let the student or the parent know that more advanced materials were available for purchase, or would that be considered "targeting" under the undefined provision of SOPIPA?

Would operators be able to promote books to parents of young readers, including books the student might enjoy based on preferences they've expressed?

Schools have long advertised products and services that are likely valued by parents and students based on activities and school programs: ads related to musical providers to members of band and orchestra; sports equipment or opportunities advertised to students of various athletic teams; scholarship ads to juniors and seniors, both for local opportunities, and perhaps more long distance options not otherwise easily discoverable.

---

[59] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf
[60] https://www.networkadvertising.org/2013_Principles.pdf
[61] http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf
[62] https://www.networkadvertising.org/2013_Principles.pdf

Without a clear definition of targeted advertising, it is unclear to operators where the line falls between these traditional and accepted ads and inappropriate use of personalized information now available in greater detail via students' digital records. To ban advertising broadly risks depriving students and parents of information and opportunities they expect and desire.

Persistent Identifiers and Advertising:

SOPIPA includes "persistent identifiers" in its definition of covered information, and as such, such identifiers may not be used for "targeted advertising." However, SOPIPA doesn't take into account the most common mechanisms by which advertising is served online, and the reasons behind those mechanisms.

Persistent identifiers come in several formats, with many dependent on the device itself and not necessarily the user. They serve a variety of purposes, including many that are for the convenience of the user. A persistent identifier is what allows the user to customize their site content and have those preferences retained the next time they visit. It is also what allows the user to retain their progress over time.

When it comes to advertising, persistent identifiers aren't just used to serve ads, they're also used to *restrict* ads. For example, persistent identifiers are used to place a cap on the number of times a user sees ads. They're also used to ensure that users don't see the same ads repeatedly.

Operators can use persistent identifiers to ensure that ads that meet the regulatory and self-regulatory requirements for children are served to children, and that ads not appropriate for children are served only to older users.

Under COPPA, the FTC acknowledges that – unlike all other personal information - persistent identifiers may be collected without prior parental notice or consent when used only to support specific internal operations, including serving contextual advertising and capping the frequency of advertising.[63]

So what does SOPIPA intend to restrict? Certainly, the second half of the clause, which is a ban on "targeted advertising on any other site, service or application when the targeting is

---

[63] *Support for the internal operations of the Web site or online service means:* (1) Those activities necessary to:
(i) Maintain or analyze the functioning of the Web site or online service; (ii) Perform network communications;
(iii) Authenticate users of, or personalize the content on, the Web site or online service; (iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising; (v) Protect the security or integrity of the user, Web site, or online service; (vi) Ensure legal or regulatory compliance; or (vii) Fulfill a request of a child as permitted by §312.5(c)(3) and (4); (2) So long as The information collected for the activities listed in paragraphs (1)(i)-(vii) of this definition is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.

based on any information, including covered information and persistent unique identifiers, that have been acquired because of the use of that operator's site service or application" is well-defined. Retargeting to students and parents is entirely prohibited. However, whatever is actually meant and enforceable with respect to the ban on "targeted advertising" alone remains unclear.

What are some of the consequences of such restrictions?

It's difficult to overstate the adverse impact of student data privacy legislation in which key provisions are undefined. However, one area to consider are the potentially unintended consequences that could result. There are many with SOPIPA.

Since "covered information" is defined so broadly and "targeted advertising" is undefined, some advocates interpret SOPIPA as imposing a complete advertising ban. A ban on even contextually relevant advertising would prohibit providing potentially useful and desirable opportunities, and potentially restrict self-directed learning and parent-guided progress.

In addition, colleges would not be able to promote admissions only to junior and senior students, or to students who otherwise undermatch at a particular institution. In a product that includes levels for multiple grades, it would prove nearly impossible to prevent younger users from seeing advertising intended only for older audiences, and vice versa. Organizations – even nonprofits or foundations – interested in reaching eligible students with scholarships would not be able to take advantage of technology to reach those students who meet certain requirements. Promotion of traditional school activities, such as selling class rings, yearbooks, class photos and more could be stifled.

However, since "targeted advertising" remains undefined in SOPIPA, it will be important to look at how the California Attorney General's office chooses to interpret and apply the clause over time.

C. What Can Parents Authorize?

Over the last two years, public concerns about student data collection have grown. Policymakers have responded to those concerns by proposing new state and federal legislation to address a variety of possible risks. Some advocates worry that sensitive data will be sent to state or federal authorities for uses they do not consider appropriate. Some are concerned that student records will be used in a discriminatory manner by colleges or future employers. Some worry that schools or vendors will sell or improperly share student data. Basic concerns about both schools and vendors simply having adequate privacy and security measures in place must be addressed by responsible stakeholders, but unfortunately some of the reactions to these concerns have unnecessarily limited parents' rights to authorize disclosure or use of their children's information. SOPIPA is an example of this overreach – which has been at least ameliorated in many of the bills modeled on it.

Federal and state lawmakers sought ways to implement and enforce student privacy laws to ensure protection of student data. In 2015, there were over 180 student privacy bills[64] under consideration in 46 states, up from the previous year record of 110 student privacy bills proposed in 36 states. In addition, in 2015, the U.S. House of Representatives[65] and U.S. Senate[66] each proposed legislation directed at ed tech vendors as well as drafting rewrites or proposed amendments to the Family Educational Rights and Privacy Act (FERPA) to update the responsibilities of schools and educational agencies.[67]

FERPA is founded on a parent's right to access their child's education record. Many bills sought to ensure or expand parental access to data in the new context of school-vendor partnerships, responding to worries that these data weren't covered or that data held by vendors wouldn't also be accessible to parents.

However, to address concerns about data being further shared with data brokers or unauthorized parties, many bills – including SOPIPA – broadly ban a vendor from sharing student data with any additional third parties. SOPIPA has no provision for parents to consent to uses of their child's data for purposes precluded by SOPIPA.
When advised that vendors were typically directed by schools or parents to send data to colleges or scholarship or financial aid organizations, some legislators amended bills in other states to include provisions allowing vendors to share data with those recipients only, with the permission of the schools or parents. However, any other transfer of student data

---

[64] Data Quality Campaign. "Student Data Privacy Legislation: What Happened in 2015, What Is Next?" (n.d.): n. pag. 24 Sept. 2015. Web.
[65] "Messer, Polis Introduce Landmark Bill to Protect Student Data Privacy." N.p., 29 Apr. 2015. Web. 12 Nov. 2015.
[66] S.1788 - 114th Congress: SAFE KIDS Act. Text. N.p., n.d. Web. https://www.congress.gov/bill/114th-congress/senate-bill/1788/text
[67] H.R.3157 - 114th Congress: Student Privacy Protection Act." Text. N.p., n.d. Web. https://www.congress.gov/bill/114th-congress/house-bill/3157/text?resultIndex=1

is frequently still banned. These bans create a significant barrier for a wide range of beneficial uses of data that parents and students want to enable.

With all the extracurricular and specialized opportunities available online, there are an increasing number of areas where parents may want to use data from or about their child to support activities outside of the school's curricular programs. They may want to make their child's data available to a tutoring program, to a college mentoring program or other educational support services.

Under SOPIPA, the parent cannot do so. Even with explicit parental request or permission, the vendor is forbidden from disclosing the student's data to the designated third party. This lack of a parental choice option to share data limits every parent's ability to make the best choices for their own child.

The law authorizes parents to download or obtain physical copies of the file or account data, but the language denies the ed tech company the ability to directly share it, even with the parent's request or consent. This puts the transfer burden on the parent, may open security concerns and can close off avenues to ensure that the information will be used effectively and efficiently. Without that ability for parents to request electronic transfer or access from those vendors who may be able and willing to provide it, the parent and student are forced to essentially start from scratch each time they start a new program outside of school.

This may become particularly relevant for children with disabilities or learning challenges who are some of the "power users" of multiple resources beyond the school. Students with physical or educational challenges usually have what are referred to as "thick files" – a great deal of information built up over time which is critical to their academic and personal success. Today, this information exists electronically. Transitioning to new or added services without the ability to easily integrate existing information creates a tremendous burden on parent and provider when each new program may have to reassess and freshly establish or document the child's abilities and requirements.

It's critical that new legislation consider first, what are the real – not the imagined – adverse privacy and security issues with student data, what are schools appropriately resourced and empowered to act around that data, how does technology really work, what are vendors truly doing (and not doing) with the data, and what do parents and students need to best support each individual's education pathway.

D. What are "Reasonable Security" Procedures and Practices?[68]

This checklist is designed to provide a simple baseline of security principles and practices as an ed tech business grows its products and services. This list of tips does not constitute a complete security policy, but if followed, will ensure that vendors have taken the best, first steps toward responsible protection of student data, as these tips flag many of the common key concerns.

1. Risk: Data Interception
Solution: Encrypt Data in Transit

End-user network traffic is easily monitored or intercepted on open WiFi or over the wire by the operator of the network. To prevent sensitive information from being accessible to unintended parties, use HTTPS (SSL/TLS). Do not send passwords in clear text! (Also encrypt data at rest; see 4. below)

2. Risk: Vulnerable Software
Solution: Regularly Patch and Update Software, Servers and Endpoints

Many data breaches are caused by the exploitation of vulnerabilities for which there are known fixes. In other words, the breach didn't have to happen. Require appropriate personnel to patch and update systems, quickly, routinely, programmatically, and often, in accordance with policy. Commonly, operations personnel apply patches, and version updates, while security analyst/engineers run scans to confirm that patching has been applied and vulnerabilities are remediated. (Keeping the distinction between the two roles provides a check and balance within the process.)

3. Risk: Database Compromise (Injection Attacks)
Solution: Use Accepted Secure Coding Practices

Code can masquerade as data, and the resulting "injection" attacks are the source of many data breaches. Thankfully the necessary secure coding practices to prevent injection attacks are well known, such as parameterized queries and sanitizing inputs. See SQL Injection Prevention Cheat Sheet.

4. Risk: Lost or Stolen Laptops and Workstations
Solution: Require Full Disk Encryption

Require your security team to use full-disk encryption on all laptops and workstations. All information at rest in your control should be encrypted. This includes your servers, third party servers, but especially when it lives on a machine that can be tucked under an arm and carried out the door. If you use or allow portable storage media (thumb drives, any

[68] https://ferpasherpa.org/s-p.html#security

portable media), they should also be encrypted. Train employees to report lost or stolen equipment immediately.

5. Risk: Password Compromise
Solution: Deploy 2-factor authentication.

Require development teams to deploy 2-factor authentication on web-accessible log-ins. Yes, this is not always possible, or practical. Strive for it where possible; when it is not feasible, employ strong password rules and controls; apply practices appropriate to the level of risk of the data involved.

6. Risk: Relying on Hashing to De-Identify Data
Solution: Use Properly Salted Hashes

Although many hash outputs or "digest" values inputs cannot be easily reverse-engineered to determine the hash input, calculating look-up tables for certain types of uniform data is very easy.

For example, a look-up table for all U.S. phone numbers can be calculated very quickly and used to look up "hashed" phone numbers. The solution is to use salted hashes and consult with a computer scientist to verify strength of resulting de-identification.

7. Risk: Cloud Services (reminder, there is no "cloud" – it's just someone else's computer)
Solution: Do Your Due Diligence.

Determine if you can even use a cloud solution based on legal requirements. If you don't encrypt student data before it is sent to the cloud, the cloud provider has physical access to the data.

8. Risk: Third-Party Management and Hosted Solutions
Solution: Due Diligence and Contractual Constraints

Your responsibility and authority for data in your possession/control extends to its management while under the control of a third party providing you a service.

Contractual constraints:

- Seek third party audits or audit reports
- Verify insurance requirements and comply
- Include relevant reps and warranties
- Require incident response provisions

9. Risk: Browser Compromise Through Java Plug-In
Solution: Disable the Java Plug-In in all Browser Software Enterprise-Wide
Never Publish Software that Requires the Java Plug-in to be Installed in Order to Run

Many instances of browser compromise occur because of security issues with the Java Plug-in for browsers. Block and disable the plug-in.

10. Risk: Other Browser and App Compromise
Solution: Require In-House and External Developers to Satisfy the Appropriate ASVS Standard

Consider using the ASVS standards – the aim of the OWASP Application Security Verification Standard (ASVS) Project is to normalize the range in the coverage and level of rigor available in the market for Web application security verification using a commercially-workable open standard. The standard provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection. See https://www.owasp.org/images/5/58/OWASP_ASVS_Version_2.pdf.

Additional Areas to Address for Security Policy and Practices

- Incident response planning and preparation: have a breach response plan. Your contract may require it, but regardless, you should have (and test, and train for, regularly) your procedures for how to respond in the event of a breach, of different magnitudes
- Insurance
- Establish, update and regularly conduct training for employees, both those directly involved in security systems and those who simply need to understand their own responsibilities
- Employ a system or process for logging and monitoring of all activities

Additional Resources

- *https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet*
- *https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business*
- *https://www.ftc.gov/datasecurity*