Future of Privacy Forum
Student Online Personal Information Protection Act 101

In recent years, over 300 student data privacy bills and laws have been introduced across the states as legislators have attempted to solve real or perceived gaps in student data privacy protections.

Of all of these, the Student Online Personal Information Protection Act (SOPIPA) of California is significantly different from legislation that has come before, in that it applies directly to operators and directly addresses data use in advertising.

California has always led the charge on enacting forward-leaning data privacy regulation, and SOPIPA is no different. Once it was passed, other states began crafting their own SOPIPA-like regulations, and that trend continues to this day. For this reason and more, SOPIPA is worth a close and careful review by every company doing business in the K-12 education sector.

What Is 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 touted by California State Senate President Pro tempore Darrell Steinberg (D-Sacramento) as a law that "fosters innovation and protects kids' privacy."[i]

It is unlike any other in terms of subject matter, reach and influence on other state legislation across the country.

It is written quite broadly, providing new and extensive data privacy protections for K12 students in California. At its core, SOPIPA has several aims, including to:

- Prevent unauthorized disclosure of certain student information
- Restrict targeted advertising to students and their parents
- Ensure that reasonable security measures are in place to protect student information
- Ensure that operators delete student information upon request by the school or district.

SOPIPA is complemented by the privacy of pupil records provision of the California Education Code[ii] (AB 1584), which authorizes educational agencies to contract with third party technology providers. AB 1584 requires that contracts between vendors and school systems specify what measures a technology provider will take to ensure the security and confidentiality of pupil records and how the technology provider and educational agency will together ensure compliance with the Family Educational Rights and Privacy Act (FERPA). Contracts that don't align with AB 1584 can be considered void.

With SOPIPA, these two laws create a comprehensive suite of data privacy regulations for student data.

SOPIPA At-a-Glance:

SOPIPA prohibits operators of websites or online services from:

1. Knowingly engaging in targeted advertising to students or their parents or legal guardians
2. Using what is referred to as "covered information" to amass a profile about a K-12 student
3. Selling student information
4. Disclosing covered information, except in specific, limited circumstances

SOPIPA requires operators of websites or online services to:

1. Implement and maintain reasonable security procedures and practices, appropriate to the nature of the covered information
2. Protect information from unauthorized access, destruction, use, modification or disclosure
3. Delete a student's covered information if the school or district requests such deletion

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.

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 design, purpose and marketing of the product.

What are K-12 School Purposes?

These are purposes that:

- customarily take place at the direction of the K-12 school, teacher or school district; OR
- aid in the administration of school activities, including:
    - instruction in the classroom or home
    - administrative activities
    - collaboration between students, school personnel or parents; OR
- are for the use and benefit of the school.

In this regard, SOPIPA applies to operators of products that are used not only in schools, but also for school activities that take place in the home.

SOPIPA does not appear to apply to operators who self-identify a product as "educational," but who have no real intention that it be used for school purposes. This means that products designed by entertainment operators and labeled as "educational," but marketed only to children or parents would not likely be covered by SOPIPA.

Operators in the education sector will not have any such exception, nor will any operator who markets a product for school purposes.

What Information Is Protected Under SOPIPA?

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.

In sum, covered information means personally identifiable information or materials, regardless of media or format that meets any of the following criteria:

- Is created or provided by a student, or the student's parent or legal guardian, to an operator 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
- Is 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
- Is 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

What are the Specific Requirements of SOPIPA?

Under SOPIPA, operators may not:

1. 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
2. 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 purposes
3. Sell a student's information, including covered information[iii]
4. Disclose covered information except in specific, limited circumstances.

What is Targeted Advertising?

This question has been the subject of much discussion and debate, as "targeted advertising" is not defined in SOPIPA or elsewhere. Existing federal regulation, industry self-regulation and guidance works off of the following terms instead:

- **Behaviorally targeted advertising** (also referred to as only behavioral advertising [OBA] or interest-based advertising) has been defined by the Direct Marketing Association (DMA) as the "collection of information about online activities and Web viewing behaviors, over time and across non-affiliate websites, to deliver tailored ads."[iv] In general, this means that a party will serve ads to a user based on the computer's browser activities over time and across different websites and online services. This definition has largely accepted by the FTC as described in the Self-Regulatory Principles for Online Behavioral Advertising.[v]

- **Contextual targeting** (also referred to as contextually relevant advertising) is defined by the DMA as advertising in which the ad served is based on a single visit to a web page or a single search query.[vi] The FTC echoes this in policy statements and in comments surrounding the Children's Online Privacy Protection Act.[vii]

Some will argue that SOPIPA intends to preclude all advertising – to students and parents - when the advertising is based on any information about a student user.

However, a critical piece here will be how California interprets this section of the law and the way it's constructed. Do we read the clause, "based upon information, including covered information and persistent unique identifiers that the operator has acquired because of the use of that operator's site, service or application" to be attached to the preclusion against both targeted advertising within the operator's product AND targeted advertising on other sites, online services and applications? Or do we interpret it to refer only to targeted advertising outside of the product, as a strict reading would suggest?[viii]

- In the former scenario, SOPIPA would impose unprecedented advertising preclusions on technology providers intending to do business in California. The resulting economic impact could be significant for companies wishing to support education in California.

- However, if we look at the latter scenario, a reasonable definition of "targeted advertising," based on foundational regulatory guidance and precedent described above would provide strong protections on personally identifiable information while allowing some advertising within products.

It would still prevent the use of any information gleaned within the operator's product to target ads to the user on sites, services and applications outside of the product. This, in and of itself, is significantly restrictive when we consider that it precludes advertising to the student users as well as to the parents and legal guardians.

Additional SOPIPA Requirements:

Operators must:

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

What are Reasonable Security Procedures and Practices?

To answer the question of what can be considered reasonable security, it's helpful to look at enforcement actions related to data security by the Federal Trade Commission. Future of Privacy Forum offers a series of Security Quick Tips for Vendors which, while not intended to fully answer the question for operators, offers a solid start on the fundamentals.

When Can an Operator Disclose Covered Information?

Covered information may be disclosed only:

1. To further the K-12 purpose of the site, service or application, provided that the recipient:
    i. Does not then disclose the information unless to allow or improve operability and functionality within the student's classroom or school; and
    ii. 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*
2. To ensure legal and regulatory compliance
3. To respond to or participate in judicial process
4. To protect the safety of users or others or the security of the site
5. To a state or local educational agency, including schools and school districts, for K-12 school purposes, as permitted by state or federal law
6. To a service provider, provided the operator contractually:
    i. 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
    ii. Prohibits the service provider from disclosing any covered information provided by the operator with subsequent third parties
    iii. Require the service provider to implement and maintain reasonable security procedures and practices as described above.

Working with Third Parties:

Before working with a third party vendor who might receive covered information, conduct due diligence on their privacy and security practices. Be sure that the vendor can comply with your

privacy and security requirements, and put contractual restrictions in place limiting their use of covered information to only what is allowed by SOPIPA.

Note that the Student Data Privacy Pledge already requires that "vendors with whom student personal information is shared in order to deliver the educational service, if any, are obligated to implement these same commitments (as are outlined in the Pledge) for the given student personal information." In addition, §312.8 of the Children's Online Privacy Protection Act makes it clear that operators must "take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner."

SOPIPA adds to that by putting a more direct prohibition on redisclosure of information, and by requiring that all of the restrictions be laid out in a contract.

How Can Operators Use Student Information?

As is the case with most student data privacy regulation, SOPIPA does allow operators to use information to maintain, develop, support, improve or diagnose their site, service or application. SOPIPA also allows operators to use student data, including covered information, for adaptive learning or customized student learning purposes.

In addition, operators may use student data to conduct:

1. Research:
   SOPIPA allows operators to conduct legitimate research, defined as:
   a. Required by state or federal law and subject to the restrictions under applicable state and federal law
   b. 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. Under the research exception, covered information may not be used for advertising purposes or to amass a profile on the student.

2. Product improvement, marketing and development:
   Operators may use deidentified student covered information:
   a. Within any of their own sites, services or applications to improve educational products.
      i. Aggregated, deidentified student covered information may be shared for the development and improvement of educational sites, services or applications
   b. To demonstrate the effectiveness of the operator's products or services, including in their marketing

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: Do You Comply With SOPIPA?

Operators will hear this question often from schools and districts in California. While SOPIPA applies to technology providers, schools and districts aim to ensure that operators comply with SOPIPA before engaging.

A few districts in California have issued guidance to schools. However, it is important to note that none of the existing guidance has been written with benefit of input from the State of California, which will ultimately determine the proper interpretation and application of SOPIPA. While the form of the guidance varies, it is often written to presume that technology providers are not compliant.

> Common Sense Media, which was instrumental in drafting SOPIPA, notes in its guidance to schools that "private educational technology companies can collect massive amounts of sensitive data about students, including contact information, performance records, online activity and keystrokes, health records, behavior and disciplinary records, eligibility for free or reduced-price lunch, family demographics and financial status, and even cafeteria selections and location along bus routes. Some edtech companies have collected and analyzed students' personal details without clear limits on how that data is being used. Others have failed to adequately secure and encrypt students' personal information from potential misuse. Preexisting federal and state laws have failed to keep up with technology and left large gaps in the protection of students' information. And many vendor contracts, terms of service, and privacy policies fail to protect student data on their own."
>
> Common Sense Media notes that SOPIPA ensures that technology providers can't use student data "to make a quick buck," and further opines that "in an educational setting, it is better for students and parents if the law bars commercial use of student data outright…"[ix]

Guidance available from the Los Angeles Unified School District[x], 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."

The assumption is that, as an operator, you are probably doing something wrong.

What Can Operators Expect When Working with California Schools?

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

Several districts have begun requiring 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 are not being written with keen knowledge of the requirements, so mistakes are common.

- One district checklist notes that vendors "must" disclose student information when required for legitimate research purposes, even if research is not part of the services being provided. That same district does not allow operators to correct mistakes on the

form, or to strike language that is not applicable to the product. The district also does not allow the use of aggregated, de-identified data for the purposes cited in AB 1584.

- Another district now requires compliance with the entire California Education Code, which 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, instead of only the AB 1584 provisions.

Still, others remain entirely unaware of the law.

Remember that many of these districts do not have privacy policies on their own websites, and they are not being told what the law actually means. Your patience, knowledge and guidance will be needed in order to ease the fears and help in crafting legally enforceable contracts.

How Will SOPIPA Be Interpreted and Enforced?

California is a vanguard when it comes to privacy. The state constitution guarantees a right to privacy[xi], and Californians can boast of a matrix of online privacy laws protecting their data. When it comes to interpreting the laws, in the past, the Attorney General's office has been reluctant to issue guidance that goes beyond the four corners of the paper. When the California Online Protection Act (CalOPPA) was amended in 2013 to include Do Not Track technologies, the Attorney General's office issued non-binding recommendations[xii] to assist operators in compliance efforts. We should expect nothing different here

One challenge for the Attorney General's office with SOPIPA will be that – unlike with CalOPPA where most terms were defined in the law – the critical term of "targeted advertising" remains undefined in SOPIPA. The law provides for the aggressive privacy protections we are used to seeing from California, but the guidance will need to be crafted carefully to avoid economic impact and reduction in technology services to schools.

When it comes to enforcement, SOPIPA was enacted under the California Business & Professions Code, which means that penalties will probably fall under the "Unfair Competition" section. Under the Code, unfair competition is defined in part to include "any unlawful, unfair or fraudulent business act or practice." The Attorney General's office, district attorneys and some city and county attorneys may be able to file suit. Students and parents will have a private right of action under the law.

The Code allows for preventative relief and civil penalties, which are calculated by the court in part by considering elements such as the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth. Intentional violations are subject to higher civil penalties, and when the nature of the conduct is "of a continuing nature," each day of that conduct is counted as a separate and distinct violation."[xiii]

What States Are Following California's Lead?

Eleven states have passed laws that resemble or take inspiration from SOPIPA:

Arkansas HB 1961 ~ Delaware SB79 ~ Georgia SB 89 ~ Maine LD454 ~ Maryland HB298 ~ Nevada SB463 ~ New Hampshire HB520 ~ Oregon SB187 ~ Virginia HB1612 ~ Oregon SB187 ~ Washington SB5419

At the same time, 44 additional bills have been proposed across 22 states that resemble SOPIPA. 15 of those bills across 8 states were proposed in 2016, a number that is likely outdated by the time you read

this. Not every bill 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.

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 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 authoritative regulatory guidance that emerges from California and other states to interpret the finer points of the laws.

---

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

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

[iii] Student information acquired by an operator prior to a purchase, merger or acquisition must remain subject to this protection by the operator and any successor entity. (SOPIPA Section 1, Chapter 22.2 (a) (3))

[iv] http://www.dmaresponsibility.org/privacy/oba.shtml

[v] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

[vi] http://www.dmaresponsibility.org/privacy/oba.shtml

[vii] https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf "Contextual advertising is ''the delivery of advertisements based upon a consumer's current visit to a Web page or a single search query, without the collection and retention of data about the consumer's online activities over time.' *See* Preliminary FTC Staff Report, 'Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,' (Dec. 2010), at 55 n.134, *available at http://ftc.gov/os/2010/12/101201privacyreport.pdf.* Such advertising 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."

[viii] "(1)(A) Engage in targeted advertising on the operator's site, service, or application, or (B) target advertising on any other site, service or application when the targeting of the advertising is based upon any information, including covered information and persistent unique identifiers, that the operator has acquired because of the use of that operator's site, service, or application described in subdivision (a)."

[ix] https://www.commonsensemedia.org/kids-action/impact/sopipa/an-introduction-to-sopipa

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

[xi] "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." (https://oag.ca.gov/privacy/privacy-laws)

[xii] https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf

[xiii] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=17001-18000&file=17200-17210