Cooley

October 9, 2014

California recently passed the first state law in the nation that comprehensively addresses student privacy. The **Student Online Personal Information Protection Act** ("SOPIPA" or "Act"), which will become effective on January 1, 2016, applies to websites, applications and online services, prohibits the use of targeted advertising, and mandates security measures which may require the encryption of data at rest and in transit.

Parties subject to SOPIPA

SOPIPA applies to operators of websites, online services, or mobile applications ("Service[s]") who have "actual knowledge" that the Service is (a) being used for K-12 school purposes and (b) "was designed and marketed for K-12 purposes" ("Covered Services"). "K-12 school purposes" is defined in the Act as any purposes that customarily take place at the direction of a K-12 school, teacher, or school district, or aid in the administration of school activities, including instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school.

SOPIPA does not apply to general audience Services, even if login credentials created for a Covered Service may be used to access those general audience Services.

One item that remains an open issue, given the broad definition of a Covered Service under SOPIPA, is whether the law will apply to online services which are intended to assist high school students identifying potential institutions, complete college applications, and calculate college costs and financial aid options. Arguably, these services—which are generally aligned with the traditional duties of school guidance counselors—could be deemed Covered Services. Covering these activities under SOPIPA would significantly expand the universe of impacted service providers.

Whether the universe of Covered Services will be better defined through regulation or guidance to include college admissions and financial aid marketing and counseling is unclear at this time. However, businesses providing such services to high school students should closely monitor developments on this issue and may ultimately need to obtain guidance if the definition of Covered Services is not clarified prior to SOPIPA's effective date.

Although SOPIPA is a California law, it will apply to operators of Services who are not California residents if they will be collecting Covered Information from California Students.

Information protected by SOPIPA

SOPIPA protects "Covered Information," which includes personally identifiable information or materials, in any media or format that meets any of the following:

- Is created or provided by a student, or the student's parent or legal guardian, to an operator of a Covered Service (a "Covered Operator") in the course of the student's, parent's, or legal guardian's use of a Covered Service 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 a Covered Operator; or

- Is gathered by a Covered Operator through the operation of a Covered Service and is descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

Actions SOPIPA prohibits

The Act prohibits the following actions:

Restrictions on advertising and profiling:

- Engaging in targeted advertising on the Covered Service using Covered Information or information obtained by a party subject to SOPIPA;
- Targeted advertising elsewhere using information collected or created (including persistent unique identifiers) using a Covered Service;
- Use of information (including persistent unique identifiers) created or collected on Covered Services for the purpose of creating a profile about students, except in furtherance of K-12 school purposes.

Restrictions on disclosure of Covered Information:

- Selling Covered Information (except in connection with merger or acquisition where acquiror is also bound by SOPIPA).
- Disclosure of any collected or created information about a student unless made in furtherance of the K-12 purpose of the Covered Services where the information is not further disclosed unless to allow or improve functionality within the student's classroom or school (except as required by law, judicial process, or necessary to protect safety of others or security of the Services). However, disclosures may be made to service providers that are contractually obligated: (1) not to use any Covered Information for any purpose other than providing the contracted service; (2) not to disclose any of the Covered Information; and (3) to implement and maintain reasonable security procedures and practices compliant with the statute.

Security and deletion requirements

SOPIPA imposes the following security and deletion requirements on Covered Services:

- **Security requirements:** Covered Operators are 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, or disclosure. Because best practices surrounding security measures have not been specified by the Attorney General, there are no clear indications as to what security measures will satisfy these obligations. Furthermore, because security requirements undergo continuous change, the standard for satisfying these obligations will continue to change as well.
- **Deletion requirements:** Covered Operators are required to delete Covered Information if the school or district requests deletion of data under the control of the school or district.

Consequences of noncompliance

Although the Act does not contain enforcement provisions, it is expected that SOPIPA will be enforced through California's Unfair Competition Law (the "UCL")[1]. Under the UCL, the California Attorney General, district attorneys, and some city and county attorneys can file suit against businesses for acts of "unfair competition," which are considered to be any act involving business that violates California law. As a result, once SOPIPA becomes effective, violations of SOPIPA may be considered violations of the UCL. Government officials bringing suit for violations of SOPIPA may seek civil penalties and equitable relief under the UCL. In addition, the UCL provides that the private plaintiffs may assert private claims for violations of the California Business & Professions Code[2].

What SOPIPA permits

The Act permits the following uses of Covered Information:

- Covered Operators may use Covered Information for "maintaining, developing, supporting, improving, and diagnosing" purposes related to the Covered Services.
- Covered Operators may also use Covered Information for legitimate research purposes as allowed by state or federal law and under the direction of a school, school district, or state department of education (and in compliance with the above restrictions on creating of profiles and advertising).
- Covered Operators may use de-identified data within the Covered Services to improve educational products or to demonstrate the effectiveness of the Covered Services.
- Covered Operators may share de-identified and aggregated student information for the development and improvement of educational sites, services, or applications.
- Covered Operators may use student data, including Covered Information, for adaptive learning or customized student learning purposes.
- Covered operators may market educational products directly to parents so long as the marketing does not result from the use of Covered Information obtained by the Covered Operator through the provision of Covered Services.

Differences from FERPA

What may be most unique about SOPIPA, for website operators with experience in the ed tech sector, is the fact that it imposes direct liability on those operators. This is in stark contrast with the most well-known educational privacy law—the Family Educational Rights and Privacy Act ("FERPA") which is enforced by the U.S. Department of Education ("DOE"). FERPA, as ed tech companies and schools know, is only directly enforceable against educational institutions receiving federal funds (which ends up being most schools). Even if a third party website operator causes a FERPA violation, DOE may only hold the school liable. Any liability by the website operator would be through its contract with the school. This shifting of the direct liability does change the analysis for website operators, but could have some benefits as well from a client relations perspective given the natural fear many schools have related privacy laws.

The enforcement ability and likelihood of SOPIPA is another area where it diverges significantly from FERPA. Private plaintiffs do not have a private right of action under FERPA. Thus, only the DOE may bring a claim against an educational institution for a violation. The potential penalties associated with a FERPA violation are potentially catastrophic for institutions. Due to both of these reasons, FERPA penalties are virtually never applied. Because SOPIPA appears to have less draconian penalties and because it provides a private right of action, enforcement actions are more likely as compared to FERPA.

Practice tips

Effective January 1, 2016, every operator of every website, application or online service that has actual knowledge that its service is being used for K-12 school purposes and if the service was designed and marketed for K-12 purposes will be required to comply with SOPIPA if it is collecting Covered Information from any K-12 students who are located in California. As a result, it is important that Covered Operators take steps over the coming year so that they are in compliance with SOPIPA by January 1, 2016. We recommend all website operators that collect information from K-12 students take the following steps.

- Determine whether your online services are Covered Services under SOPIPA.
- Conduct an audit of your online services to determine whether your services collect any Covered Information. If so, put into place procedural and technical measures designed to ensure the information is not used for any of the restricted purposes or otherwise disclosed in violation of the law.
- Conduct a threat and risk assessment (TRA) to determine what security measures would be appropriate for your particular service.
- Employ technical, physical, and administrative security measures commensurate with the sensitive nature of the applicable Covered Information. This may include (a) developing new and/or revising existing policies and procedures and (b) using industry best practices such as encryption to protect the data both in transit and at rest on your services.
- Determine whether your services were designed for K-12 Purposes. If so, be cautious about using the information obtained through such services and ensure that any use of this information is in compliance with this law.
- Review your existing agreements with subcontractors and consider amending existing and/or future contracts to require subcontractors to comply with SOPIPA. Consider whether indemnification by your subcontractors may be appropriate. Similar FERPA provisions are also advisable.

NOTES

1. Cal. Bus. & Prof. Code §§17200-17209.
2. Id. §17204.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090