SOPIPA Overview

Summary

The **Student Online Personal Information Protection Act (SOPIPA)** is a California state law (Cal. Bus. & Prof. Code § 22583–22587) enacted in 2014 and effective January 1, 2016, designed to protect the online privacy of K-12 students by restricting how operators of websites, online services, and mobile apps collect, use, and disclose student personal information. It addresses gaps in federal laws like FERPA and COPPA by prohibiting non-educational commercial uses of student data, such as targeted advertising or profiling, while allowing legitimate educational purposes. SOPIPA promotes a trusted digital learning environment without explicit enforcement penalties, relying on California's Unfair Competition Law (UCL) for remedies like civil penalties or injunctions. It has inspired similar laws in other states (e.g., Illinois' SOPPA) and federal proposals.

Key Requirements

SOPIPA imposes specific prohibitions and obligations on covered operators to safeguard "covered information" (broadly defined as any data that identifies or describes a student, including names, addresses, emails, grades, test results, biometric data, geolocation, photos, voice recordings, search activity, and more). Key requirements include:

1. **Prohibitions on Use and Disclosure**:
    - No targeted advertising on the operator's site/service/app or elsewhere, based on covered information or persistent unique identifiers.
    - No using covered information to create, maintain, or amass a profile about a student for non-K-12 school purposes.
    - No selling a student's covered information.
    - No disclosing covered information to third parties unless for K-12 school purposes, legal compliance (e.g., court order), or with a contract ensuring continued SOPIPA compliance.
2. **Security and Deletion Obligations**:
    - Implement and maintain reasonable security procedures and practices to protect covered information from unauthorized access, destruction, use, modification, or disclosure (may include encryption at rest and in transit).
    - Delete a student's covered information upon request from the school or district.
3. **Permitted Uses**:

    - Covered information can be used for K-12 school purposes (e.g., instruction, administration, collaboration) or to maintain, develop, support, improve, or diagnose the service.
    - Marketing educational products directly to parents/teachers is allowed if not based on covered information from the service.
4. **Scope Exclusions**:
    - Does not apply to general-audience sites/services/apps, even if accessed via school credentials.
    - No parental consent can override prohibitions on commercial uses.

Enforcement: No private right of action for individuals without demonstrable harm; enforced by the California Attorney General under UCL (potential civil penalties up to $2,500 per violation).

Who Is Affected

- **Operators**: Providers of websites, online services, online applications, or mobile apps with "actual knowledge" that they are used by K-12 students in California for school purposes (e.g., edtech companies like Google Classroom, Khan Academy, or custom learning apps). Applies even if the operator is based outside California but serves CA students.
- **Schools and Districts**: K-12 public/private schools, teachers, and districts in California; they can request data deletion and must ensure vendor contracts align with SOPIPA.
- **Students and Parents**: K-12 students (up to grade 12) in California whose data is collected via school-directed online services; parents/guardians benefit indirectly through protections but cannot consent to prohibited uses.
- **Third Parties**: Vendors or affiliates receiving disclosed data must comply with SOPIPA-equivalent protections.
- **Impact of Non-Compliance**: Potential UCL lawsuits by the AG (fines, injunctions); reputational damage; no direct student/parent lawsuits unless harm (e.g., financial loss) is proven. Affects the edtech ecosystem by requiring privacy-by-design in student-facing tools.

Relevance to Scholarships: If your scholarship platform collects K-12 student data (e.g., essays, transcripts via school partnerships in CA), you must avoid using it for non-educational purposes and comply with deletion requests. (Clarification: SOPIPA applies only when collecting data from California K–12 students.)

Informational Resources

- **Official California Legislative Text**: Full bill (SB 1177) and code at leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22583 (free; includes definitions and prohibitions).
- **California Attorney General's Guide**: "Ready for School: A Guide to Student Privacy in the Digital Age" (oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/ready-for-school-1116.pdf)—comprehensive overview with FAQs, checklists, and vendor contract tips.
- **Future of Privacy Forum (FPF) Guide**: "Protecting Student Data Under SOPIPA" (fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf)—detailed compliance toolkit with examples on targeted advertising and actual knowledge.
- **Common Sense Media**: SOPIPA explainer and advocacy resources (commonsensemedia.org/kids-action/about-us/our-issues/digital-life/sopipa)—includes differences from other laws and edtech impact.
- **EFF Legal Overview**: eff.org/issues/student-privacy/legalanalysis—compares SOPIPA to federal/state laws like FERPA/COPPA.
- **Additional Tools**: Parent Coalition for Student Privacy (studentprivacymatters.org/state-legislation/) for state comparisons; TermsFeed blog (termsfeed.com/blog/sopipa/) for practical implementation.