SCHOOLS LEGAL SERVICE

LAW UPDATE
SCHOOL BUSINESS

PHONE: (661) 636-4830 • FAX: (661) 636-4843
E-mail: sls@kern.org • www.schoolslegalservice.org

December 4, 2014

STUDENT/TECHNOLOGY BILLS FROM 2014

The Legislature recently passed three bills which were signed by Governor Brown (two of the bills take effect in January 2015 and the third doesn't go into effect until 2016). These three technology-related bills are summarized below. Two of the bills relate to cloud computing and online privacy protections, the subject of our breakout session at the August Workshop this year.

AB 1442 - Pupil Records, Social Media

This bill imposes certain obligations and restrictions on school districts, county offices of education, and charter schools that elect to monitor student social media outside of school, and extends those obligations and restrictions to companies contracting with an educational agency to provide those monitoring services.

Agencies can gather or maintain only social media information that directly pertains to student or school safety and must destroy that information when the student has not been enrolled in the agency for one year, or upon the student reaching the age of 19, whichever comes first.

The destruction obligation is different for third-party vendors of monitoring services. The agency must give the vendor notice when the pupil turns 18 or is no longer enrolled with the agency, upon which notice the vendor is to reasonably act to destroy the information. The vendor is to immediately destroy the information upon satisfying the terms of the monitoring contract.

Contracts with third-party vendors of monitoring services must contain provisions that prohibit use of the information for any purpose other than to satisfy the purpose of the contract and prohibit selling the information or sharing it except to the agency or to the pupil or pupil's parent or guardian.

If an agency is contemplating adopting such a program, it must give notice to students and their parents/guardians of such intent and provide an opportunity for public comment at a regularly scheduled public meeting of the agency's governing board or body.

Any program adopted by the agency must contain provisions for access to the information by the pupil and/or parent/guardian, including an opportunity to correct or delete information, and the agency must give notice to parents or guardians that the information is being collected. This notice can be in the Annual Notice to Parents and must include an explanation of the process

for requesting access to, correction, or deletion of the information. Nothing in the bill indicates the correction or deletion of any collected information is mandatory, except as to the destruction time limits.

AB 1584 - Privacy of Pupil Records in Third Party Contracts for Cloud Services

This bill recognizes the increasing frequency of educational records and services being stored and/or occurring "in the cloud" (meaning agencies are online and data is increasingly electronic). The bill permits such activity, setting minimum standards for protection of pupil records, access to such records, notifications of security breaches, and limitations on retention of the records on completion of the contract.

Most significantly, the bill prohibits third-party vendors from any use of any information in pupil records that is not expressly required or permitted by the contract. This provision impacts the ability of vendors to offer free or low cost services, which have traditionally been provided in the expectation that data gleaned from the records would have commercial value to the vendor. While this provision sounds like a significant protection, it is only a mirror of the existing impact of federal FERPA rules and the bill specifically excludes "deidentified" pupil information from the definition of protected pupil records. This also mirrors existing law.

The bill attempts to preclude targeted advertising but links the prohibition to advertising arising from use of personally identifiable information in the pupil records. For instance, vendors are not prohibited from targeted advertising based on information gathered from other sources, for example, from the pupil's use of a free application ("app") offered by the same vendor, or shared by an affiliate, outside the school environment. The terms of service (TOS) that pupils agree to before accessing the free "app" quite often indicate the vendor will be collecting and sharing data from the pupil's use of the product, and the pupil, or teacher, agrees to that use by accepting the TOS and using the app. This highlights the significance of the education agency having a comprehensive Acceptable Use Policy, one that prohibits or limits unapproved and/or outside software, including apps, from being loaded onto agency technology and prohibits or limits the use of personal devices if they contain such software.

Still, the bill is a step in the right direction: a contract is now required and certain provisions are mandated for inclusion in that contract, and the absence of or defects in the terms of a contract for such services renders the contract void if the deficiencies are not corrected.

SB 1177 - Student Online Personal Information Protection Act

This bill, which does not become effective until January 1, 2016, is intended to protect the privacy of some information collected online, prohibits targeted advertising on Internet websites, online services, and apps used primarily for K-12 purposes (defined as those that customarily take place at the direction of the school, the teacher, or district, or aid in the administration of activities, including instruction, whether in the classroom or at home, or in administrative activities or collaboration between students, school personnel, or parents). The bill applies to sites and services provided to districts, county offices of education, and charter schools.

This bill applies to providers of Internet websites, online services, and apps, including

mobile apps, and also prohibits targeted advertising on other sites, services, or apps operated by the provider if based on any information the provider obtained by providing the online K-12 services. However, the bill does not apply to general audience Internet sites, services, or apps. It prohibits providers from using any information to amass a profile about a K-12 student, unless in furtherance of a K-12 school purpose, and from selling a student's information.

Any disclosure of covered information is prohibited unless required in furtherance of a K-12 school purpose, or required by law or to protect the safety of users or others, or the security of the site, or for a service provider who is subject to the same restrictions. However, information may be used by the provider for internal purposes of maintaining, developing, supporting, improving, and diagnosing the provider's site, service, or app, or for adaptive or customized student learning purposes, if this is part of the purpose of the site, service, or app. As with FERPA, use of deidentified data is permitted to improve the vendor's educational products or demonstrate the effectiveness of their products, including use in their marketing, but this permitted use does not include targeted marketing to students.

Additionally, providers must implement and maintain reasonable security practices and procedures, appropriate to the nature of the information, to protect against unauthorized access to information, and delete agency information if requested by the agency. Students may download, export, or save their own data and documents.

Protected information includes personally identifiable information in any form or format that is created or provided by a student or an agency employee, or is gathered by the provider's operation of the site, service, or app, if it is descriptive of or identifies a student. The bill's definition of protected information is at least as broad as that of FERPA regulations, as it includes information in email and text messages, student records, information that allows physical or online contact, socioeconomic data, food purchases, search activity, photos, voice audio, location, and includes the term "documents" without further definition.

This does not mean providers may not monitor and/or collect information via their site, service, or app; only that subsequent use and disclosure is limited. This is illustrated by the following example: Disclosure may be made when in furtherance of the safety of users or others or the security of the site. Presumably, this would permit reporting collected information to the K-12 agency if the information discloses a safety risk, such as a threat. Just why or how the information would come to the attention of the provider is unknown, unless providers are monitoring and/or collecting information.

This bill protects sensitive information that can be collected via some form of Internet usage in an agency's educational program. Since online educational programs are becoming more commonplace, the bill is timely. It also illustrates the risks that come with use of the Internet, especially when personal devices are permitted to be used in the agency's online educational program.

While the collection and use of online data by K-12 program providers are controlled under this bill, the collection and use of the same data by other, non-K-12 services, apps, and the like that may be present on the personal device are not controlled. There is a likelihood of such services and software apps being present on the personal devices, and they are infamous for their collection and use of data obtained via the downloading and use of their products, all of which are

permitted via agreement to their TOS. So while the intended K-12 uses may protect data, the uncontrolled presence of data mining apps and the like still put such data at risk. Parental consents and/or waivers should be considered along with controlling the use of personal devices in the educational program.

If you have questions concerning any of this information, please don't hesitate to contact our office.

— *William A. Hornback*

Education Law Updates are intended to alert clients to developments in legislation, opinions of courts and administrative bodies and related matters. They are not intended as legal advice in any specific situation. Please consult legal counsel as to how the issue presented may affect your particular circumstances.