LAW UPDATE
SCHOOL BUSINESS

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

June 22, 2016

TECHNOLOGY: VOLUME 1

I. CLASS ACTION LAWSUITS OVER COLLECTING AND SHARING BIOMETRIC DATA

Courts in Illinois are litigating multiple class action lawsuits over collecting and sharing biometric data including retina scans, fingerprints, voiceprints, and the like. Under the Biometric Information Privacy Act (BIPA) entities that collect such data must have written consent and written retention policies. Targets of the class action lawsuits include Facebook and Shutterfly for the alleged collection of facial images; other actions involve using fingerprints in place of membership cards. In one case, a plaintiff alleges Shutterfly used facial recognition software to identify him without his consent and without his ever having used Shutterfly. While BIPA expressly excludes collection of photographs from its coverage, at least one court has ruled that excluding photographs does not equate to the exclusion of identifiable facial features derived from the photographs.

For educational agencies, biometric data is protected as personally identifiable information under FERPA, where it is defined as:

> "Biometric record," as used in the definition of "personally identifiable information," means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

Accordingly, collection, storage, and use of biometric data should be carefully monitored and controlled. This includes controlling the use of biometric data in the classroom (where using pictures and audio and other data is commonplace) along with online programs and mobile apps (e.g., Facebook and Shutterfly) that may not be approved or controlled by the educational agency and which may be collecting and sharing that data during their use in the classroom. All of this is done under the authority of "click-wrap" Terms of Service to which teachers and students routinely agree without review.

II. FTC AND OTHERS PURSUE APP DEVELOPERS AND TOY MANUFACTURERS OVER ALLEGED COPPA VIOLATIONS

The FTC has collected fines from various app developers for collecting minors' "persistent identifiers" through use of their apps on the minors' devices without providing adequate notice to and consent from the minors' parents and then sharing the collected data with third-party advertisers. Fines can be up to $16,000 per violation.

Educational agencies typically comply with the Children's Online Privacy Protection Act (COPPA) by making online service providers "school officials" to whom information may be properly released. There are arguments that parents' consent to such release is given when the Annual Notice is signed and returned each year. Absent appropriate criteria and status as a "school official," an online provider may allege the agency is the party obligated to obtain the written consent. This is problematic for agencies that have online services and mobile apps in classroom use without the agency's knowledge or consent. Absent appropriate contractual arrangements to establish a "school official" status, collection and disclosure of student identifiers may be both FERPA and COPPA violations. COPPA violations already result in financial penalties, and FERPA is being amended to permit financial penalties for FERPA violations.

In related news, toymaker Mattel was recently sued for online collection of voiceprint data via its "Hello Barbie" doll. While the online collection feature is not activated until an adult registers the device and consent, all done in efforts to comply with COPPA, the allegations in the lawsuit are that the voiceprints of the user's friends are also being collected online without any consent on the part of their parents. Does much online sharing of protected information occur in your classrooms? Does your Acceptable Use Policy include parental consent for the disclosures?

III. IS YOUR WEBSITE ADA COMPLIANT?

The Department of Justice recently indicated it will delay proposed rulemaking on access to Internet websites for disabled users until 2018. In the meantime, it appears the Web Content Accessibility Guidelines propounded by the World Wide Web Consortium (W3C) are the standard. Those guidelines appear at https://www.w3.org/TR/WCAG20/.

The W3C guidelines include references to the following standards. Website content should be:

Perceivable: Provide text alternatives for any non-text content so it can be changed into other forms people need, such as large print, braille, speech, symbols, or simpler language; provide alternatives for time-based media; create content that can be presented in different ways (for example simpler layout) without losing information or structure; make it easier for users to see and hear content including separating foreground from background.

Operable: Make all functionality available from a keyboard; provide users enough time to read and use content; do not design content in a way that is known to cause seizures; provide ways to help users navigate, find content, and determine where they are.

Understandable: Make text content readable and understandable; make web pages appear and operate in predictable ways; help users avoid and correct mistakes.

Robust: Maximize compatibility with current and future user agents, including assistive technologies.

Lawsuits around the country have inconsistent results as to whether a website is subject to the ADA. The federal Court of Appeals for the Ninth Circuit (the court with jurisdiction over California) held that a "public accommodation" within the meaning of the ADA means an actual, physical place. The Seventh Circuit has found websites to be public accommodations. Even courts within the Ninth Circuit have found a nexus between a website and a physical location (Target stores and Target.com) for ADA purposes.

Given the increasing significance of public agency websites to their communities and the increasingly common statutory obligations to post various items on public websites, the need for access to the information for all members of the public is increasing. This may spur lawsuits where a website is not accessible. In recent years a single law firm specializing in ADA compliance lawsuits has issued hundreds of demand letters related to website access.

In a recent California case, a retailer was found liable for damages because the retailer's website was inaccessible to a blind plaintiff. Liability was found to rest on both federal and state law, including the Unruh Civil Rights Act in the California Civil Code. Mitigating accommodations included having a website designed to be read by screen reading software. It does not appear a plaintiff is required to request that accommodations be made before filing a lawsuit; it appears sufficient if they can type in your URL and not be able to use your website.

IV. DATA BREACH COVERAGE FOUND UNDER TYPICAL COMMERCIAL GENERAL LIABILITY POLICY

In April the federal Court of Appeals for the Fourth Circuit found an insurance company had an obligation to defend its insured for alleged breach of data security resulting from inadvertent posting of patient medical records on the Internet. While this situation involved medical records, there are similar arguments that would arise in circumstances involving student records, especially if the records contained students' personally identifiable information (PII). The duty was found under the "personal and advertising injury" provisions of the policy.

The data was stored online and inadvertently made accessible and searchable by the public. This was considered a "disclosure" of the data and should raise concerns about whether school district staff members are placing student education records online, especially if they include PII. If placed online in a manner that may permit access and/or searching by persons without authorized access to the information, the school district may find itself facing allegations of student records disclosure.

As a reminder, SISC members have access to data breach coverage. Contact SISC if there are questions about coverage under various data breach circumstances.

V. MORE ON DATA BREACHES - SOME SURPRISING FACTS

The Attorney General recently released a report indicating malware and hacking posed the greatest threats to data security, followed by theft or loss of unencrypted data on personal devices and breaches by errors such as inadvertent exposure of data and mis-delivered email. Governmental agencies made half of the error-related breaches. Some sources indicate as much as 20 percent of data breaches involved paper records. Last year, a pharmacy was fined $125,000 for failing to properly dispose of paper records.

These statistics are relevant to education agencies in that they continue to:

1. Move more data into the "cloud" and away from local servers.

2. Transition away from paper to digital records, leaving significant questions about disposition of paper records.

3. Bring increasing amounts of technology into the classroom, creating increased risk of accidental disclosure of student data by other students, by the students themselves, and by invasive software/malware present on personal devices used in the classroom.

4. Expand the use of mobile apps and devices, with ever-increasing storage capacity and with an increased risk of data breach from the loss or theft of the mobile devices, some of which may have automatic access to agency servers and networks which create a portal to more data.

VI. EDUCATIONAL TECHNOLOGY CONTRACTS

Recent experience with common instructional software companies has disclosed some startling and disappointing results. Both Houghton Mifflin and McGraw Hill have recently submitted contracts to local school districts for assessment/other student metrics and for a math intervention program, respectively. Neither contract contained California's requirements for technology (cloud) contracts which have been in effect since at least January 2015. Ongoing federal efforts to reinforce student data security in the cloud are modeled after existing California statutes. Since significant amounts of personally identifiable student data are being loaded into each of these software programs/websites, and since the intent of the statutes was to protect this data, the total absence of required protective language in the contracts creates significant risk for school districts using these vendors' contracts without modification.

FERPA violations currently bear little financial risk for a school district in that a FERPA-related loss of all federal funding is a result virtually unseen in public education. However, given the current consideration of "fines" and other penalties being considered for additional remedies for FERPA violations, the future impact of software breaches and intentional data disclosures (from lack of the minimal contractual requirements) places school districts at financial risk.

Schools Legal Service has developed a chart containing contractual requirements in an easy reference format/checklist of the required components necessary to comply with California law. We also offer a contract addendum form which can be attached to and incorporated into vendors' form contracts to ensure compliance with the California Codes. Feel free to contact us for information.

VII. STUDENT PHOTOGRAPHS ON A DISTRICT WEBSITE - OR ELSEWHERE

There is ongoing discussion about the risks to educational agencies from the ever-present smart phones and iPads, etc., with their cameras and ability to post pictures online within seconds of an event. Is the picture an educational record of a student and entitled to protection? With the coming changes to FERPA and the potential for imposition of fines for FERPA violations, there are risks for educational agencies and uncertainties about those risks.

A photograph may be an "education record" under FERPA where educational records are defined as anything "directly related to a student and maintained by an educational agency." Pictures posted to an agency's own website are maintained, as are pictures posted to agency-controlled social media. Photographs can be educational records as FERPA regulations include them in the list of records that can be considered to be "directory information." While photographs can be directory information, and disclosure of directory information is not typically a FERPA violation, parents can opt out of having directory information regarding their child published, making a disclosure where parents have opted-out a violation.

Publication of student photos on staff or student personal websites or social media could be an unauthorized disclosure as well. While the agency should exercise control over those actions by students and staff, the ability to discipline students and staff for unauthorized disclosure of FERPA-protected information may not be a defense against a fine imposed for that disclosure. If the disclosure resulted from an educational activity or program operated by the agency, or if the agency permitted students unrestricted access to and use of personal devices, the agency could be found at least partially at fault for the disclosure. Permission for the disclosure could be inferred from a failure to have any controls over the use of personal devices.

Another source of risk could be the known permitted use of personal devices that contain personal software and apps that are known to "mine" personal data from the devices onto which they are installed. Many of those apps openly disclose their collection and use practices in their Terms of Service, which users must accept to download the app. Those practices, and the very presence of those apps on any personal device permitted by the agency, create risk for disclosure of student records also found on those devices. One example could be the use of personal devices for agency email or social media, including student communications, when data-mining software or apps are also present on the personal device. Contact our office for recommended language discouraging those uses.

VIII. THE "INTERNET OF THINGS" AND INCREASED RISK OF UNAUTHORIZED DISCLOSURE OF PROTECTED INFORMATION

The "Internet of things" is composed of the ever-increasing number of everyday items that contain some form of online connections, from garage door openers to thermostats to cars to health products. In some parts of the world, your car already sends information to billboards which identify your car and tailor ads to you. You may recall a recent incident where hackers remotely stopped a car on the road.

Even toys involve the Internet of things. Mattel's "Hello Barbie" is one example (a child speaks to the doll, the voice is analyzed in the cloud, and an array of responses is made available). The communications are apparently recorded and stored. (Imagine a small-scale "Siri" with a change of clothes.)

A recent hack of toy manufacturer Vtech demonstrates the scope of information collected by devices in the Internet of things. The VTech hack created a leak of personally identifiable information (i.e., customer names, email addresses, passwords, and home addresses) of up to 4.8 million adults and more than six million children.

In the wake of the hack, VTech has attempted to pass along the risk of the loss of such data to consumers by including an "assumption of the risk" clause in the standard Terms of Service. Legal challenges are already being made but the results are uncertain.

Other developers of child-directed apps were recently fined by the FTC for COPPA violations for failing to obtain clear parental consent before sharing collected information from the apps with other vendors who target advertising based on the collected data.

Voice activated TV manufacturer Samsung is said to have recorded some spoken words around their television devices, in some cases without the consumer's knowledge. Samsung's Terms of Service authorized the capture and transmission of those spoken words to third parties.

Just as some of us wouldn't want everything we say in front of our TV shared with unknown persons, unknowingly sharing classroom discussions is a significant privacy concern. The risks increase as more and more devices from the Internet of things enter the market, with the likelihood that more and more of them are also going to enter the classroom. This makes the need for careful review of the Terms of Service for all software and apps even more important for school districts.

This area is changing so rapidly that we anticipate sending another technology update very soon. Please contact us with any questions you may have in the meantime.

William A. Hornback

School Business 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.