LAW UPDATE
EDUCATION

SCHOOLS LEGAL SERVICE

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

September 18, 2017

TECHNOLOGY: VOLUME FOUR

The following is another installment in our ongoing effort to track technology trends and foresee applications in the education setting.

I. Website Access Update

Thanks to Bret Holthe, Director of Technology at Fruitvale School District, who shared Fruitvale's OCR experiences with us at the breakout session at this year's August Workshop. Bret has indicated that OCR is still moving forward on existing claims and Resolution Agreements (RA), albeit slowly. While holding districts to the timelines imposed on them in an RA, OCR often seems to allow their own timelines to slip when getting approvals back to the districts. This has made the process longer but not necessarily increased the work or cost.

Bret also said that districts should continue to work on problems and his first recommendation was to find an auditor early, as that person/agency could also provide guidance on finding other necessary tools and support. Bret reported that the third party web design companies that commonly serve K-12 education are diligently working to restructure their website designs and functionality. This will be a genuine boon to districts receiving letters from OCR in the future. Bret confirms our belief that the obligation to become and remain ADA compliant is not going to go away.

We are researching whether OCR has actually adopted the WCAG 2.0 AA guidelines and standards or is merely pushing them unofficially. We understand the US Access Board has adopted the WCAG standards, but we also understand those rules only apply to federal agencies and contractors. We also note that the Department of Justice, the primary commercial enforcement agency of access rules as to commercial entities, has withdrawn regulatory efforts to adopt the WCAG standards. You may recall that it was the DOJ's inability to adopt actual standards that a court used to dismiss a website access action against Domino's Pizza (a topic in an earlier Tech Update). Those unadopted, draft regulations have now been dropped by the DOJ. Accordingly, the issue is still quite fluid so stay tuned for another update.

In the meantime, we note that educational agencies are still experiencing fallout from ADA access issues. One recent incident involved UC Berkeley where ADA access issues were the reason the university took down over 20,000 free videos and podcasts from its YouTube and iTunes

channels, thus removing public access to those resources. While we have been advised that it is not OCR's intent to force districts to take down or limit their websites, that is becoming a clear option for those agencies with massive websites. While the absence of regulatory requirements has been used as a defense, it doesn't stop OCR from making claims and it could be expensive to defend against claims by the federal government. We continue to recommend efforts to comply at the WCAG 2.0 AA level.

II. Google Action on Apps

In March Google started removing various Apps from its marketplace Google Play. The Apps reportedly were removed for various reasons involving privacy policies and data security. Google requires transparency in the Apps marketed through Google Play, especially if they collect personally identifiable, financial, payment, contacts, or other sensitive information from consumers. One of Google's requirements for Apps is that the privacy policy be posted in the Google Play listing of the App and within the App itself. It is unknown how many of those Apps were previously accessible via links from inside G Suite.

On a related matter, we understand Google has made changes to its G Suite core App (called "Hangouts") and this is causing concern about privacy and confidentiality. We understand the changes to include the ability to link and share data/images with those outside the agency's network. While communication with the outside world is, at times, helpful and desirable, there is no apparent way to instantly clear those outsiders as "school officials" entitled to receive confidential student data. For this reason, some agencies are turning off Hangouts for student use until a solution is found.

In more Google news, their most recent newsletter (September 8) indicates that teachers and administrators can get up-to-date information on Google education programs via YouTube videos. Of course, YouTube isn't one of the G Suite core Apps and isn't subject to any enhanced privacy rules. While the data of teachers and administrators isn't subject to FERPA or California's K-12 cloud computing restrictions, and therefore of less concern, Google is also pushing a tool for teaching students on the subject of privacy and claims the tool will ". . . engage students and teach them how to explore the online world in a safe, responsible, respectful way." The tool is on YouTube, the non-core App.

III. Data Issues with Health and Fitness Apps

The New York Office of the Attorney General recently settled with several mobile Apps that purport to help monitor users' health and fitness, often using a smartphone. In addition to claims of misleading advertising, allegations included that the Apps relied on user consent by default. The settlements provide that the Apps must require express user consent to share data, they must clearly state they are not medical devices, and they must include express notice that medical information collected may not be protected under HIPAA. Additionally, the settlements require notice that aggregated data collected by the App could be shared and individual users be reidentified by recipients of that data.

Do you know if similar devices are being used in your classrooms? While medical information often finds its way into student records, that information is typically classified as FERPA protected rather than HIPAA protected. If any of these Apps are in use in the classroom, any medical information collected by the App could fall within the rules of HIPAA which are significantly more strict than FERPA rules.

IV. Cyberhacking School District Information

The Miami-Dade County Public Schools and the Manatee County School District in Florida are both being sued or threatened by employees and students whose confidential information was hacked. One district lost employees' W2 information via a "phishing" scheme and the other actually posted student standardized test scores and Social Security numbers on the district's website. Googling two students' names found the disclosed information, which implied an even broader dissemination of the data. Those two students filed suit and lawyers also filed a complaint alleging FERPA violations with the US Department of Education.

These incidents highlight the need for significant training for those posting district website content. Add this to the need for special posting to make the content accessible to those with disabilities and a "website poster" position appears to be a new job classification for public education.

V. Cloud Vendors as the Weak Link in Data Security?

In mid-July it was reported that a Verizon vendor misconfigured a cloud server resulting in information on six customers becoming exposed online. While this may be a relatively isolated incident, it highlights the potentially massive impact a data breach may have on educational agencies. It may be that the vendor would be obligated to indemnify the educational agency but educational agencies own the data in the cloud and it is their responsibility to keep it safe.

Typical data security recommendations made by experts (i.e., written contracts, adequate security, and immediate notice of breach) are already part of California law. Contracts are required and must include reasonable descriptions of the efforts taken by cloud vendors for data security. It is also believed that cloud vendors providing educational software, web-based learning, cloud-based student databanks, etc., are already focused on data security and provide adequate precautions.

The risk to education is from the use of small, often mobile, Apps less prepared to deal with advanced cyberhacking efforts and often using third party storage to support their operation. The third party may not be fully prepared to protect data to the level expected by the educational agency, although the vendor may be obligated by contract to do so. If the vendor fails to select an adequately secure storage provider, the educational agency is still the primary target of breach claims.

VI. Movement on Risks in the IoT

As reported in earlier volumes, the internet of things (IoT) has some strange and scary household items that collect data from their owners, sometimes without the owners' knowledge.

Currently pending SB 327 would impose restrictions and obligations on manufacturers of devices intended to be connected to the internet.

Among the new requirements, the manufacturer must include notice about whether a device collects personal information (such as audio, video, location, biometric, or health data), as well as how the information is collected and how often, on the device's packaging or on the manufacturer's website. Consumer consent is required before the data can be used or transmitted beyond what's required for the device to function.

Consent may be revoked but there is no indication in the bill whether consent is opt-in/ opt-out. A prior version of the amended bill required the device to have some indication of when it was collecting data. SB 327 has been made a two-year bill, so activity on it will continue in the next legislative year.

VII. Don't Open that Personal Email

A Maryland federal court has ruled that the personal email account of an employee is not subject to search by an employer, and that searching the personal email violates the Stored Communications Act (SCA). While the court's logic in the case is complicated, it is clear that any unopened email in a personal account would be subject to the SCA and the employer opening the email would be in violation of the Act. There are complex arguments about whether or not opened email remains subject to the Act, but in Maryland the action was permitted to go forward even as to emails allegedly already opened.

Accordingly, we are advising employers to be very careful about accessing personal email accounts. In the Maryland case, the personal account was on an employer-owned device, turned in at when employment terminated.

VIII. GPS Tracking Devices . . . Again . . . and Worse!

It has come to our attention that some students may be coming to class with GPS tracking devices in their backpacks or on their clothing, with the school not being asked to consent to the device's use. As we have noted in the past, the primary but not only problem with GPS devices is the common component of voice recording/transmitting that accompanies the device. There are several privacy concerns as to other students and staff, as well as the potential criminal issues with unapproved recording devices in the classroom.

Not only are GPS devices an issue, we are now experiencing an increased number of Apple watches at school with the voice function activated and parents or others listening in to the classroom, playground, lunchroom, restroom, and other locations as if on a phone call. Contact us if you are experiencing this phenomenon.

As always, please feel free to contact our office if you have questions concerning these or related issues.

— William A. Hornback

Education Law Updates are intended to alert Schools Legal Service 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. Consult legal counsel as to how the issue presented may affect your particular circumstances.