LAW UPDATE
EDUCATION

SCHOOLS LEGAL SERVICE

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

May 22, 2017

TECHNOLOGY: VOLUME THREE

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

I. Data Privacy

The "Internet of Things" (IoT) continues to collect horror stories about connected devices creating unforeseen, or at least unwanted, consequences. From toys to helpful home devices to medical devices, the IoT is creating awareness of privacy issues.

A good example is the "My Friend Cayla" doll from the Vivid Toy Group. According to complaints to the FTC, the doll's bluetooth connection is subject to hackers who can listen to and even talk to a child. Although known since early 2015, the software problem had not been fixed as of February 2017.

"Cayla" is not the only toy to have issues. It was reported earlier this year that Spiral Toys, makers of the "Cloud Pets" toy series, makes a stuffed Internet-enabled bear that could be hacked using only a smartphone from anywhere within 10 meters, or farther if a directional antennae is used; a hacker could leave up to five messages of 40 seconds duration. One hacker with a smartphone reportedly directed a stuffed unicorn to broadcast "exterminate, annihilate, destroy." It may also be possible to extend the length of the messages since the software was not encrypted or protected. To make matters worse, it was also reported that the cloud network supporting the toys was left unsecured, without a firewall or even password protection, exposing the log-in credentials of over 800,000 users to theft.

In another incident, the FTC recently required smart TV manufacturer Vizio to pay a $2.2 million fine for tracking the content viewed on Internet-connected TVs and smart monitors. It was alleged the tracking capabilities of the smart TVs permitted third parties to analyze viewing habits, assess audience size, determine the effectiveness of advertising campaigns, and deliver advertising based on the information collected, none of which Vizio disclosed. The FTC complaint considered television viewing history as sensitive personal information. While uncontrolled television viewing is not, hopefully, a daily occurrence in schools, smart TVs may be in use and the capabilities and restrictions on the plentiful "Smart Boards" used by schools may need to be reviewed for legal compliance.

In another example from the IoT, we note that data collected from an individual's pacemaker has been used in a criminal investigation. Following a cardiologist's review of data captured from the pacemaker, the cardiologist indicated the data didn't match the individual's description of his actions at the time of a fire. The individual has been charged with aggravated arson and insurance fraud.

While people love being able to remotely control devices, play music, and get news updates, those conveniences come at the price of family privacy. Alexa (the "personal assistant" from Amazon) is always listening.

II. Data Security

We all know there are ongoing investigations into alleged Russian involvement in the recent presidential election. The U.S. Justice Department recently charged Russian intelligence officers and others with involvement in the September hacking of Yahoo, a hack which compromised personal information of roughly 500 million people. Of greater concern however is that the hackers then used the information they obtained from the Yahoo hack to access Yahoo, Google, and other webmail accounts. Approximately 1 billion Yahoo accounts were hacked in December.

The FTC has also issued guidance on "cross-device tracking" which is information obtained from one device being linked to other devices used by the same user. While there is no prohibition against collecting cross-device information, the ability of technology to match bits of data and link it to the same user has created results like a search on one device resulting in targeted advertising on that subject appearing on the user's other devices.

In an odd twist to "phishing email" problems, an Illinois student is suing his high school for expelling him following failed attempts to change his grades. The student was alleged to have participated in a scheme to use a fake email from PowerSchool to set up a fake website to collect login credentials of teachers who fell for the phishing scam. While the attempt to change his grades ultimately failed, the district felt the significant amount of time it spent to resolve system issues, and the loss of trust in the accuracy of the district's grading system, was sufficient harm to warrant the expulsion. The student has now sued, arguing expulsion was too harsh a punishment.

Recent incidents involving phishing emails, taken together with hackers' use of stolen passwords, are leading to increased data security efforts including recommended changes to an agency's Acceptable Use Policy (AUP) for both staff and students. We point out that small agencies are targets (as are large companies) in part due to small agencies often having fewer protections in place.

Given the risks and limited funding, employee training is said to be one of the best tools currently available to guard against intrusions. It is recommended that employees be trained to watch for phishing schemes and malware-laden email from unknown sources. With the amount of stolen data already out in the world, along with some of the most recent mass breaches, indications are that hackers are using stolen data to access other accounts of the victims, often made possible by the number of single-password users who use the same password on every account. Now cross-device tracking indicates that additional protective action may be needed. Breach of one account, including access to the account password, often tells hackers where the person works. If

the victim uses the same password at work as at home or on personal devices, hackers may find easy access into the victim's work network, other accounts, and devices.

While we recommend that all passwords should be both robust and unique, this is especially so with agency account access. The post-hack use of stolen information to access additional accounts has resulted in revisions to the SLS recommended AUP by placing additional requirements for password protection in both district network connections and in any personal devices which may contain agency information (e.g., laptops, tablets, iPads, and smartphones).

While the current recommendation is to have all of these devices password protected, the new recommendation is that those passwords each be different from the others, and especially different from the passwords used on personal email, social media, and other accounts and devices. At least having different passwords would make the access to district accounts and devices more difficult for hackers. The latest SLS version of an AUP includes this as a requirement for employees and recommends it for use in an upgraded student AUP.

III. Website Access Update

Last year, SLS reported that over 250 commercial companies have been sued since 2015 for lack of ADA website compliance. While education agencies are well aware of the efforts by Office for Civil Rights to force website access compliance by education agencies, both governmental and private parties are pursuing lawsuits against commercial companies. Compliance with the Web Content Accessability Guidelines (WCAG) 2.0 AA standards remains the minimum target goal of federal agencies in both educational and commercial arenas. There are due process bills pending in the House of Representatives intending to give commercial companies the right to attempt to cure alleged defects in their websites before being sued by a private individual.

In related news, the U.S. Architectural and Transportation Barriers Compliance Board recently adopted the WCAG 2.0 AA standards as the design standard for all federal agency and contractor websites. While the Department of Justice (DOJ) has been pushing for adoption of the same standards and using them as measuring tools in complaints against private companies, the DOJ has not begun the process to formally adopt final regulations to that effect. The final regulatory process is not expected to begin until sometime in 2018, but the settlements entered into by the DOJ involve those standards.

While the government continues to assert that compliance with the WCAG standards is mandated, the federal District Court for the Central District in California recently ruled against a claimant seeking damages for the inability of the Domino's website and/or mobile app to be used by blind/visually impaired individuals. The court found that the allegations against Domino's, without a "fix" having been adopted by the DOJ, violated Domino's due process rights.

The court granted Domino's motion to dismiss the lawsuit, without prejudice, pursuant to the primary jurisdiction doctrine (which allows courts to dismiss a complaint without prejudice pending resolution of an issue within the special competence of an administrative agency). The court noted that seven years had passed since the DOJ started the process to adopt standards for website compliance. In slamming the lack of action, the court noted:

> "Congress has vested the Attorney General with promulgating regulations clarifying how places of public accommodation must meet their statutory obligations of

> providing access to the public under the comprehensive ADA. Congress has further provided that the DOJ's mandate with respect to Title III of the ADA is 'to issue implementing regulations, see 42 U.S.C. § 12186(b), to render technical assistance explaining the responsibilities of covered individuals and institutions, § 12206(c), and to enforce Title III in court, § 12188(b). . . . Such regulations and technical assistance are necessary for the Court to determine what obligations a regulated individual or institution must abide by in order to comply with Title III. Moreover, the Court finds the issue of web accessibility obligations to require both expertise and uniformity in administration, as demonstrated by the DOJ's multi-year campaign to issue a final rule on this subject. See Clark, 523 F.3d at 1115."

The court concludes by calling on Congress, the Attorney General, and the DOJ to take action to set minimum web accessibility standards for the benefit of the disabled community, those subject to Title III, and the judiciary.

While the claims made in this action against a commercial company are not identical to the claims being made by OCR as to educational agencies, the rationale of the primary jurisdiction doctrine should apply to both DOJ and OCR jurisdiction should an educational agency decide to fight instead of entering into a resolution agreement.

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.