SCHOOLS LEGAL SERVICE

LAW UPDATE EDUCATION

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

February 23, 2017

TECHNOLOGY: VOLUME TW0

In ongoing efforts to track technology trends and foresee applications in the education setting, we offer this update on recent technology news.

I. Schools Do Not Typically Violate the Telephone Consumer Protection Act When Sending Home Auto-Dialed or Pre-recorded Informational Messages

The Federal Communications Commission (FCC) has determined that school districts' auto-dialers and pre-recorded messages are not violations of the Telephone Consumer Protection Act (TCPA). The TCPA precludes certain uses of auto-dialers and pre-recorded telemarketing messages and solicitations for commercial purposes.

On request from Blackboard, Inc. (an educational vendor involved in automated messages), the government took information from various educational agencies including DC public schools, Chicago public schools, and LAUSD. Blackboard asserted the informational messages from schools were the kinds of messages parents wanted to receive on their wireless devices and are distinguishable from commercial telemarketing solicitations.

In opposition, some comments indicated that the TCPA does not treat informational calls differently from telemarketing calls in protecting wireless consumers from robocalls. The National Consumer Law Center argued that low-income consumers who have limited minute plans must be protected from unwanted calls by restricting emergency calls to true emergencies.

The FCC determined that typical educational informational contacts do not violate the TCPA. Typical contacts include both wireless calls and text messages, usually for attendance messages, emergencies such as school lock-downs, fire and weather warnings, and outreach messages such as teacher conferences. The wireless contacts were deemed to be made with express consent, thus outside the TCPA, where the wireless number has been given to the school for contact purposes.

The FCC confirmed that school callers may make auto-dialed calls and send automated texts to student family wireless phones, without express consent, for emergencies including weather closures, fire, health risks, threats, and unexcused absences; however, the FCC declined to extend the TCPA's "emergency purpose" exception to every automated call made by an educational

organization. In 2016 the FCC determined that since text messages come within the jurisdiction of the TCPA, similar rules apply to auto-dialed text messages as those applicable to auto-dialed phone calls.

The FCC also granted additional relief for those calls and messages that are closely related to the school's mission (such as notice of a teacher conference or general school activity). In doing so the FCC made clear that absent evidence to the contrary, those calls are made with the express consent of the parent who provided the number. Such non-emergency automated calls and texts are lawful if the caller has the consumer recipient's prior consent. FCC rules and orders do not require any specific method for obtaining consent for the auto-dialed or recorded calls, and the FCC acknowledged that in some cases merely giving out the number implies consent to receive messages closely related to the purpose for which the consumer gave the number, further indicating the scope of consent must be determined upon the facts of each situation.

II. "Do Not Track" Update

In recent updates and presentations on the ongoing issues with website access for vision and hearing impaired individuals, we have indicated that the World Wide Web Consortium (W3C) has website access compliance guidelines that the Department of Justice, Office for Civil Rights, ACLU, and others accept and recommend. A link to those guidelines is:

https://www.w3.org/standards/techs/wcag#w3c_all

W3C is now also indicating that progress is being made on "do not track" standards so Internet users will have more control over online tracking by third-parties. Tracking by first party websites (those with whom the user has intentionally connected) can still track users and collect data, as permitted by the website's privacy policy and terms of service (TOS). The April 2016 version of the W3C work is available using the following link:

https://www.w3.org/TR/2016/CR-tracking-compliance-20160426/

California law currently requires commercial cloud vendors to indicate their practices with regard to "do not track" requests from individual web browsers. They are not required to accept a "do not track" request.

III. Security Within The "Internet of Things"

The National Institute of Standards and Technology (part of the U.S. Department of Commerce) has published an extensive paper on security guidance related to "interconnected devices" including the Internet of Things (IoT). A link to that guidance is:

https://www.nist.gov/node/1119866

The federal government's concern is indicative of the risks associated with the growing world of interconnected devices including cars, home security systems, and toys. With the presence of technology in our schools, there is an increasing security risk associated with these devices.

For example, you may recall the recent news accounts of criminal investigations involving recovery of data from a home "Alexa" system; there has also been recent activity involving "My Friend Cayla" and the "i-Que" robot which provide interactive experiences for children.

Specifically, one complaint to the Federal Trade Commission (FTC) alleges that by design the toys ". . . record and collect the private conversations of young children without any limitations on collection, use, or disclosure of this personal information. The toys subject young children to ongoing surveillance and are deployed in homes across the United States without any meaningful data protection standards. They pose an imminent threat to the safety and security of children in the United States."

Some manufacturers are alleged to assume they have parental consent because their apps are downloaded, granting the manufacturers collection and use rights. The notice to downloading individuals is buried about 3,800 small font words into the TOS. The toys also contain product placements (targeted advertising?) embedded into the software, touting Disney locations and products.

Are such devices being brought to school and shared? The complaints to the FTC allege the toys violate the Children's Online Privacy Protection Act (COPPA), collecting data from minors via Wi-Fi or Bluetooth connections without parental consent, and that those connections are capable of a "Google" search via voice recognition software also raising concerns about the non-use of filtered content, which could also be a violation of the Children's Internet Protection Act (CIPA) if occurring in schools.

IV. Data Breach Notice Requirements are Updated

Notice must be given when a data breach involving personally identifiable information occurs. School districts were excluded from this requirement until a few years ago and in 2016 another "safe harbor" was eliminated. Until AB 2828 (amending Civil Code Sections 1798.29 and 1798.82) was passed last year, a breach involving encrypted data did not require giving the notice. AB 2828 changed the rules to require giving notice if the encryption key or security credential was also breached and there is reason to believe the personal information may be readable or usable.

V. Causes of Data Breaches

While California's law on student data privacy "in the cloud" is generally ahead of the rest of the nation, it is still important to remember that data breaches impact agencies large and small, and often are associated with unintentional actions of internal personnel. There are known scams in the digital world which seek to load malware or viruses or are "phishing" for access.

Training personnel who have access to sensitive data is seen by many as an essential component of any data security plan. Training should include information on passwords and password strength, and recommendations for frequent changes. Education on the agency's process for reporting suspicious emails should also be implemented. More than anything, only employees with a need for the information should have access, and all employees should be trained on the kinds of information deemed sensitive or private, as well as on agency procedures for handling and storing that information.

Others are pointing out the risks associated with permitting personal devices to connect to any agency system containing personal information; they recommend installing software on the personal device that separates agency data from personal data and enables the agency to remotely wipe the device should it become lost or stolen.

VI. Are District Websites "Commercial" Websites?

In California, since 2004 there has been a requirement that operators of commercial websites or online services provide a conspicuous privacy policy. Known as CalOPPA, the Online Privacy Protection Act also includes requirements related to collection of personally identifying information and "do not track" requests. The law applies to commercial websites.

With the expanding use of websites by educational agencies, there is an ongoing question about whether agency websites are now subject to these rules. Is your website selling anything online (e.g., logo gear, lunch tickets, athletics tickets, or anything else)? Students and staff are already considered to be "consumers" for various purposes under California law and it isn't a difficult leap from the existing consumer status to commercial consumer status.

Schools Legal Service is currently preparing generic website TOS including privacy policy provisions for possible educational agency use. With increasing use of district networks and websites by parents, we are also working on an Acceptable Use Agreement for parents with staff and students continuing to use existing AUP options. Consider whether your district requires these items and contact us with questions.

VII. Peeking Into the Cybersecurity Future - State and National Levels

Data privacy is an ongoing concern to schools and with its former Attorney General in the forefront, California has been a leader in protecting the privacy of student data. With Kamala Harris's election to the United States Senate and the appointment of Xavier Becerra to replace her as Attorney General, along with a new FTC chairperson as well as a new President, many states are expected to continue efforts to enhance privacy rights.

The last administration received recommendations for continued and enhanced cybersecurity for both public and private interests in December 2016. Coming from the Commission on Enhancing National Cybersecurity, the recommendations included harmonizing disparate regulations across government agencies, private sectors, and internationally; moving for strong authentication beyond the password; minimum security standards for the IoT; moving security away from the end user; adopting a "cyber nutrition label" that describes the product's cybersecurity risks and features; that the FTC adopt a "Consumer Bill of Rights" covering citizens' rights and responsibilities in the digital age; and development of a "workforce surge" of 150,000 more cybersecurity practitioners by 2020.

VIII. Complaints About Complex TOS and Privacy Policy Terms

Hyperlinked TOS and contract provisions are becoming more controversial as the use of hyperlinks increases. Most cloud providers offer TOS and/or privacy policy provisions that are themselves linked from a home page, and those documents include hyperlinks to various provisions such as "acceptable use" or "privacy notice" or "support" or "apps products" or "non-apps terms" or "services" or "services level agreement" or "TSS Guidelines" or "user features" or "data privacy officer" or "data about subprocessors" or "removing content" or "data processing amendment" or "cookies and similar technologies" or "activity controls," etc.

All of these hyperlinks are found in Google's G Suite documents and they lead across multiple web pages, documents, chances for unknown changes, and multiple ways to make

inconsistent statements. Even agreements for smaller scale products sometimes contain multiple cross-references. Agencies responsible for watching the Internet are beginning to find irregularities with overly complex and repeatedly hyperlinked contract and privacy provisions, finding inadequate consent and improper data sharing. We will continue to watch the trend to see how far it goes.

For schools, the solution may be to insist that any linked pages become printed attachments to the contract so the rules, as they exist at the time of contracting, are preserved. Changes can be negotiated as laws change but this presumes there is equal footing in the negotiating world, which is not something readily achievable with some providers. The ability to change terms may be effectively zero, with the end result being "like it or leave."

For example, Google's G Suite contract documents, terms of service, privacy policy, and related documents contain numerous links to other documents which makes reviewing their contract for legal compliance more difficult. We also note that the state of Mississippi has sued Google over the G Suite products. The state claims that student data is being improperly collected and used by Google, claims that mirror our own lingering concerns. Some of the concerns stem from the requirement to use the administrator dashboard to set various privacy rights in order to comply with California law. These privacy settings are within the control of the school district but the legality of the contract may also depend on the privacy setting actually being fixed in concrete. These concerns have not been resolved and the question of legality remains.

Additionally, the G Suite core components, the ones to which the privacy policy and the multitude of other hyperlinked Google documents are said to apply, expressly do not cover use of other Google products, which may operate under rules permitting the collection and widespread use of customer data. Worse, Google indicates the G Suite core services' limitations on use do not apply to data collected from other Google products, which may be shared and combined with data legally collected from core services. It is for these reasons we recommend the strictest data sharing controls be activated in the administrator dashboard and that there be a prohibition or the inability to link to other Google products on the same devices or within the same networks where G Suite is found.

As always, we recommend you carefully read the TOS and privacy policy of any online site or service you use, and contact us for support or help with contract terms that create issues for you.

IX. The "Unknown" Creates Data Security Risk

Schools Legal Service has long been advocating that districts have some controlled gateway for technology use with rules to ensure that software and online services have been reviewed and approved, and that devices are protected and Internet connections appropriately filtered. Do your teachers use online or mobile apps in the classroom? Do you know/have you identified every one of them? We now understand that in the IT industry these risks are referred to as "Shadow IT" and its evil twin "Stealth IT."

Shadow IT consists of internal IT systems and solutions that are installed and used without express authorization; Stealth IT represents systems installed and used under authority of departments outside the IT department. Each creates the distinct possibility that student and other records are stored in a cloud that cannot be identified or located. Does the app vendor

actively mine and share student data? Does a known "mining" app exist on a Shadow IT personal device?

As with other tech issues, let us know if you need support, have questions, or contracts to be reviewed.

X. Learning From Data Breach Experiences - 2016

Baker & Hostetler LLP are advising (Blog, December 22, 2016) that data security breach experience in 2016 shows some interesting patterns. Initially they point out that regardless of the level of your security, attackers usually find a way into your system not because of your technology, but primarily due to use by real people who have flaws and make mistakes. In 2016 most breach incidents were not due to sophisticated, unpreventable attack. According to Baker & Hostetler, the most commonly found attacks involved theft of data, a surge of ransomware, and the emergence of denial-of-service arising from compromised IoT devices.

Based on experiences in 2016, steps to reduce the risk should include paying better attention to existing security measures, accepting that the system and all connected devices are not fully known to the security team and that the system contains unknown devices and unidentified third party access. Baker & Hostetler recommends actually reviewing security logs, questioning assumptions about vendors' security precautions and status, and realizing it takes the entire organization, an all-inclusive approach, to reduce risk of data breach.

Schools Legal Service believes this means agencies should look for ways to increase staff's knowledge and sensitivity related to confidential data, how it's created, and how it should be handled, and linking those to staff's obligations under the AUP. Since the future will belong to the youth of today, they too should be taught the value of data security. Information is the currency of the future, and we should all protect its value.

FINAL WORD: When looking at the cost of software and/or apps, remember that you are always paying, sometimes with money and the rest of the time with the data they take from you.

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.