LAW UPDATE
EDUCATION

SCHOOLS LEGAL SERVICE

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

September 28, 2018

TECHNOLOGY: VOLUME SEVEN

While we've all been busy and some of these "updates" are somewhat dated, they are still important to show the direction of the flow of technology into every aspect of our lives, and our jobs. Enjoy!

1. More On Password And Personal Devices

Employers are increasingly moving toward flexibility for employees, which in terms of technology means employees are working from home, using their personal devices, and resulting in the presence of confidential/protected data on a variety of personal and portable devices.

It is reported that the earliest and still the most common way data is compromised is through the loss of a mobile device, whether thumb drive, smart phone, tablet or laptop. Experts make some recommendations to minimize the impact and risks of such losses. The recommendations include:

A. As to thumb drives, to the extent allowed at all, mandate that they be encrypted and password protected.

B. As to laptops and tablets, and even home computers, require they be password protected, that passwords be frequently changed, and that any access to office networks be subject to multi-layered verification, which could include a second password only known by the intended user.

C. As to other personal devices, the recommendations include full disk encryption and the capability of remote "full-wipe" in the event of loss of control of the device.

D. Employee training and awareness are still major tools against unauthorized data access, especially as to phishing and other email scams targeting employees.

These requirements are, for the most part, already part of our recommended Acceptable Use Policy. It is unlikely that the importance of data security is ever going to be less, so keeping staff on top of the issue, through all sorts of education, is also recommended. Some agencies are testing employee susceptibility to scams. Contact legal counsel if there is interest in such testing.

2. Employee Guilty of Crime for Sabotage of Employer's Network

Using the federal Computer Fraud and Abuse Act (18 U.S.C. Section 1030), an I.T. worker was convicted in federal court of sabotaging the employer's network. The conviction was a rejection of the workers' defense that the I.T. job description included intentional disabling of portions of the system as required. The court found the Act included both unauthorized access and access in excess of authorization.

It is not unheard of for disgruntled employees to delete files and otherwise impair portions of a district's network to which the employee has access. The court in this case made it clear that federal law criminalizes intentional damage to a network, whether or not the network was hacked or accessed appropriately. The court convicted the defendant for the intentional deletion of files, among other actions. Remember this next time an employee deletes all their files on the way out.

In California, Penal Code Section 502 makes the commission of various acts involving a computer or network a "public offense constituting either a misdemeanor or felony, depending on the extent of damage," and provides the owner with a civil action including the potential for punitive damages. It appears federal law would also apply and provide remedies. Contact legal counsel if you have this occurring in your district.

3. Your Car as a Personal Device

Those of you with high-tech cars will appreciate this next part. A report indicates a security engineer found his car had captured and stored data from his phone while the car and phone were linked via Bluetooth. [Connecting the phone to the car allows bypass of Android and/or Apple security protections. Data is stored in plain text (unencrypted) on the infotainment system.] The stored data included contact lists, call logs, text messages, emails, and directory listings.

The problem is at least twofold: 1) the car's infotainment system was capable of being hacked and the information being compromised, and 2) of somewhat greater concern, given the fairly common custom of having our cars worked on at an auto shop, the data in the infotainment system can be accessed and downloaded directly via the USB port connection. Your mechanic can read your email and texts.

While there does not appear to be a current solution, car manufacturers are looking at the data security issues with their cars (think "driver-less vehicle"). At this point, we have no suggestions for revisions to your AUP, but perhaps you should consider reminding your staff that the data in the car is permanent unless deleted, which should be done when a vehicle with an infotainment system is being sold. The district does not want the vehicle's new owner to also have access to the employee's email and text messages, or photos or audio files that deal with district business or student information.

4. New Mexico Takes on Big-Tech

The Attorney General of New Mexico has filed an action in federal court seeking injunctions and recovery of investigation and litigation fees against some software companies large and small. The complaint alleges the companies designed, developed, and marketed to children under the age of 13 various mobile apps with embedded coding known as "software development kits" or SDKs, that are alleged to have collected personal data about the children to advertisers, in violation of COPPA because the data collection is done without informed parental consent. The SDKs are embedded in games and collect and share data using persistent identifiers associated with the user and the device used. The collected data is often shared, sold, and combined with data from other sources to create a profile of the child, resulting in targeted advertising. SDKs are alleged to be incorporated into over one million apps, facilitating hundreds of billions of ad requests per month and generating billions of dollars for developers in the last six years.

The lawsuit alleges violations of COPPA, New Mexico law, and a general claim for invasion of privacy filed by the state on behalf of all its residents. Targets of the lawsuit include Twitter and Google. While we are not, at this time, indicating Google's G-Suite is involved, we will take this opportunity to remind districts that Google only claims to protect student data in the "core apps" in its G-Suite product, any other Google app or product being subject to less restrictive rules.

As technology continues to develop and problems continue to arise, it appears these updates will be coming with greater frequency. Please feel free to contact us with specific questions or concerns.

— 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.