LAW UPDATE
EDUCATION

SCHOOLS LEGAL SERVICE

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

January 8, 2018

TECHNOLOGY: VOLUME FIVE

We are happy to bring you the next installment of "Everything You Need To Know About Education Technology Issues . . . And So Much More."

I. Technology Searches at the Border

A new lawsuit filed last September by the American Civil Liberties Union and the Electronic Frontier Foundation against the Department of Homeland Security seeks to stop searches without warrants of citizens' cell phones, computers, and other technology when crossing the border. On behalf of 11 individual plaintiffs, the suit alleges the policies of the Customs and Border Protection Unit permit the searches, even with no suspicion of wrongdoing, in violation of the Fourth Amendment.

The suit tests application of the Fourth Amendment at the border, with the plaintiffs' position being the Fourth Amendment applies to U.S. citizens everywhere and the Border Protection Unit asserting that the Fourth Amendment does not exist for anyone trying to cross a border into the United States.

We bring this to your attention not because your staff is going to be doing much business outside of U.S. boundaries, but because of the increasing proliferation of personal smart phones, tablets, and other portable computers in the school environment. Given 1) the increasing use, along with the commonplace practice of staff checking office email on such devices, and doing an increasing amount of office work from home (or at home), and 2) the commonplace presence of protected student or staff information in such devices, the unwarranted, unprotected, and unauthorized (by FERPA[1]) inspection of personal technology puts such information at risk of breach and inappropriate disclosure. For this reason, it was recommended that New York attorneys use "burner" phones when traveling outside the country.

[1]FERPA only authorizes release of protected information to law enforcement in response to a lawful court order or subpoena and then requires advance notice, in most instances, to the parents (34 CFR 9931(a)(9)).

Until the lawsuit is resolved, your employees should consider whether or not to take those types of personal devices across the border. An amendment to the standard Acceptable Use Policy is being considered.

II. "Big Brother" Hacked?

Also in September, the Securities and Exchange Commission (SEC) announced it had been hacked in 2016. The SEC maintains an online database called the "Electronic Data Gathering Analysis and Retrieval" (EDGAR) system to which public and other companies are required to post various corporate and compliance filings. Depending on the timing of the filings, the hack may have exposed sensitive information before it was supposed to be made public which would be the hacker equivalent to possessing "insider" trading information and give them and others with access to the hacked data the opportunity to make trades based on the information before it became public.

The "Big Brother" aspect of the hack is its potential impact on the SEC's development of the "Consolidated Audit Trail" (CAT) which is a new system designed to track each and every equity and options trade on U.S. markets and create a central repository for private trading information, a lucrative target for hackers.

After investigations into the hack, the U.S. Government Accounting Office reported concerns that the SEC failed to consistently protect network boundaries from intrusion, identify and authenticate users, authorize access to resources, audit and monitor actions taken on the system and network, and failed to encrypt sensitive information while in transmission. These are all matters with which school districts are concerned on a daily basis and the violation of which could result in breaches of pupil or other sensitive information. As your information database takes on more and more of the "Big Brother" characteristics, like EDGAR, the obligation to prevent unauthorized access increases in kind.

III. More "Internet of Things" (IOT) Developments

The Federal Trade Commission updated its guidance last fall to enhance compliance with the protections of the Children's Online Privacy Protection Act (COPPA) against unauthorized collection of data on children under age 13. The updated guidance clarifies that COPPA applies to bluetooth enabled devices that collect data (such as the dolls and stuffed animals mentioned in past tech updates). Manufacturers must ascertain the user is at least 13 years old or obtain parental consent before collecting data.

To obtain parental consent, the guidance considers asking questions to which only parents would know the answers or comparing official photo identification to other submitted photos to confirm that the submission is from the parent.

Again, the purpose of this reference is to encourage you to maintain careful watch over the devices being brought into and used in the classroom. Those devices may well be capable of collecting student information without compliance with California's online privacy protections.

IV. Copyright Infringement Subpoenas

We are all well aware of the risk of copyright infringement via the Internet to the extent that the Acceptable Use Policy has long included prohibitions against personal use of the Internet that causes any charges to the district (e.g., payments to music licensing companies for downloading/sharing copyrighted music). Enforcement against infringement went at least one step further this year when Internet service providers were served subpoenas by court order requiring the providers to identify the true names, addresses, and email addresses of each IP address subscriber alleged to have participated in illegal infringement using a peer-to-peer sharing system.

The court ordered the disclosures to enable the copyright holder to name and serve the infringement complaint on the actual defendants. This is potentially significant in that a school district may be identified by a provider and may have to identify the actual user of the IP address, meaning potentially an employee or student. We note that naming an employee or student does not necessarily insulate the district from potential liability for improper use of district technology to infringe on copyrighted material.

V. Expanding Website Accessibility Actions

In September a visually impaired individual was permitted to file a class action on behalf of all visually impaired people against Fordham University alleging discrimination because the University's website was inaccessible to the visually impaired. This "private action," which is in addition to ongoing regulatory activity by the Office for Civil Rights and the Department of Justice as to website accessibility, shows an increase in the interest and risks associated with website accessability. The action seeks injunctive relief as well as compensatory damages and attorney's fees.

VI. Biometric Privacy

We all know that FERPA protects biometric data as personally identifiable information (PII) but there has been action against social media for collection of such data without consent. The circumstances of the federal lawsuit against photo sharing website Shutterfly are disconcerting. The lawsuit contends that an individual found his photo uploaded to Shutterfly and tagged with his name although he had never used Shutterfly. It is alleged that Shutterfly then "mapped" the individual's face and stored the data without notice or consent.

The action is in Illinois, home of the Biometric Information Privacy Act (BIPA) which is said to be the strongest in the nation. BIPA requires companies collecting biometric data to obtain prior consent, disclose how the company will use the data and how long they will keep it, and allows private individuals to sue for violations of the Act.

The risk to school districts is that pupil images may be uploaded to Shutterfly or other similar social media sites and then may be mapped and stored without parental consent, which would be an unauthorized disclosure of PII and a FERPA violation. If done without an appropriate cloud contract in place, this would likely also be a violation of California law.

VII. Possible Upgrade to California Data Privacy

A potential ballot initiative is floating around California awaiting over 300,000 valid signatures to make the November 2018 ballot. Called the Consumer Right to Privacy Act of 2018, the initiative would enact additions to the Civil Code. The initiative has until May or June 2018 to verify sufficient signatures to get on the ballot.

If enacted, the initiative would provide that consumers (including you, your staff, your students) have the right to:

1. Know what information about them is being collected;

2. Compel disclosure to them of that information on request;

3. Know what information about them is being sold, and to whom;

4. Know what information about them is being disclosed to others for a business purpose, and to whom;

5. Opt out of the sale of their personal information by the business on request;

8. Be treated the same by the business, including pricing, whether or not they opt out of the sale of their personal information;

9. Contact the business through a telephone number and website, if the business has one, for the purpose of submitting requests for information without having to create an account to obtain the information;

10. Receive requested information within 45 days of a request;

11. Have a business disclose in a privacy policy or on its website a description of consumer rights and methods of submitting requests, a list of the categories of information collected about consumers in the preceding 12 months, a list of the categories of consumer information sold or disclosed;

12. Know categories of personal information collected including:

    A. Identifiers such as a real name, alias, postal address, unique identifier, Internet protocol address, electronic mail address, account name, Social Security number, driver's license number, passport number, or other similar identifiers;

    B. All categories of personal information enumerated in Civil Code Section 1798.80 et seq., with specific reference to the category of information that has been collected;

    C. All categories of personal information relating to characteristics of protected classifications under California or federal law, with specific reference to the category of information that has been collected, such as race, ethnicity, or gender;

    D. Commercial information, including records of property, products, or services provided, obtained, or considered, or other purchasing or consuming histories or tendencies;

    E. Biometric data;

    F. Internet or other electronic network activity information including but not limited to browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;

    G. Geolocation data;

    H. Audio, electronic, visual, thermal, olfactory, or similar information;

I. Psychometric information;

J. Professional or employment-related information;

K. Inferences drawn from any of the information identified above; and

L. Any of the categories of information set forth in this subdivision as they pertain to minor children of the consumer.

As technology continues to develop and problems continue to arise, it appears these updates will be coming with greater frequency. Also 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.