Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Dangers Of Data Mining, Click-Wrap And Free Apps

Law360, New York (May 23, 2014, 12:21 PM ET) -- On April 30, 2014, Google Inc. announced it will no longer scan students' email using Google Apps for Education for any potential advertising purposes. This is the latest in a startling chain of events that is playing itself out in the U.S. District Court for the Northern District of California that can have dramatic and far-reaching implications for California's schools.

In In Re: Google Inc. Gmail litigation, 13-MD-02430 LHK, Google's attorneys produced declarations admitting the free applications they have given to millions of students are used to collect advertising information to be used elsewhere on the Internet. What's more, they claim that schools must obtain user consent for this practice or potentially be liable for privacy violations. This case underscores the absolute necessity to have airtight policies, internal controls and vendor contracts concerning all online operators.

The Lawsuit: Plaintiffs Alleged That Google Apps for Education Scans Student Email for Marketing Purposes

Plaintiffs allege that Google Apps for Education, a service that provides students with basic office applications, is really being used to surreptitiously collect information for advertising and marketing purposes. "Data mining" is performed by a profiling algorithm that collects keywords and metadata to make accurate estimates about user preferences. Plaintiffs claim that the practices are nonconsensual, secretive and performed in a manner that violates basic privacy rights. Plaintiffs allege several violations of state and federal wiretap and privacy laws including the Federal Education Right to Privacy Act. The allegations are chilling enough; what is even more troubling is Google's defense.

The Defense: Users Consented to Data Collection, and If They Did Not the District Should Have Obtained Consent

Google did not deny data mining; in fact, it freely admitted that it scanned email for targeted Internet advertising even when that function is turned off. Oddly enough, the most important legal issue may not

be the “data mining” practice, but rather whether users consented to the scanning. Google presented scores of articles showing their “data mining” practices are so universally known that users must have impliedly consented. In the alternative, Google argues that schools with whom they contract, “have a contractual obligation to obtain their students’ and end-users’ consent to Google’s automated scanning.” So, according to Google, users either impliedly consented or it is the school’s responsibility to obtain the consent.

Formerly, Google had many different, and sometimes inconsistent, privacy policies for its many Web-based functions. In 2012, Google consolidated its “consumer privacy policies” into a single policy. The policy was intended to facilitate its ability to combine information extracted from its different services, such as Google Plus, Google search and YouTube, thereby enabling more comprehensive and lucrative advertisement profiling. In response to a public outcry about using student information for marketing, Google initially denied that this policy would apply to schools. It stated that its government customers have “individual contracts” that “supersede” its new privacy policy. The problem is that the standard consumer privacy policy remains an intrinsic component of the standard Google Apps for Education contract.

Court filings confirm that Google still has agreements that require obtaining “any necessary authorizations from the end user to enable Google to provide the services.” Stated differently, if districts want the service they must either obtain user consent or suffer the consequences. Alternatively, a district can negotiate an “individual agreement” that “supersedes” Google’s consumer privacy policy. But why would Google do that? If they do that for one school system, wouldn’t they have to do that for everybody? Last year in the United States, Google generated more advertising revenue than the entire newspaper industry combined. It appears highly unlikely that Google would willingly forfeit the mother lode of targeted marketing: teens and pre-teens. Realistically, how is a school going to possibly negotiate at arm’s length with Google?

The Unfortunate Truth: If School Districts Accept Free Online Services, They Risk Liability for Privacy Violations

School districts have little ability to negotiate effectively with Google. Districts either accept Google’s terms or they do not receive the service. In altering its scanning practices, Google dealt with a public relations issue, not a legal issue. Google’s lawyers are smart and they have a point. There is a contract requiring educational institutions to obtain user consent. So let this be a lesson to us all; there is no such thing as a free lunch. We should view free applications and technological panaceas with skepticism. Although it is unrealistic to expect that school staff is going to be able to consummately navigate this rapidly changing legal and technological minefield alone, there are some things that can be done to protect our students’ privacy and protect school districts in the process.

The Response: What Districts Can Do to Protect Student Privacy

Familiarize yourself with applicable law.

It is important to understand relevant law to fashion policies and agreements that comply with those laws. The Protection of Pupil Rights Amendment and the Children's Online Privacy and Protection Act, in conjunction with FERPA constitute the federal statutory scheme protecting student's online privacy. FERPA prevents the disclosure of student information. The PPRA requires that a school district notify parents if their children may participate in online activities involving data collection for marketing purposes. COPPA applies to commercial sites directed to children under the age of 13. It is important to stay abreast of changes in state and federal law in an ever-shifting legislative environment struggling to keep up with technological advances.

Establish district policies and procedures to address online operators.

School districts should remember they have an important role in setting policies to protect student privacy. Many districts already have processes for evaluating online vendor contracts for privacy and security considerations. Staff cannot bypass internal controls in the acquisition process when deciding to use online services. It is best to treat free service the same as paid services to ensure compliance with district policy.

Districts should establish board policies for selecting online educational services. These policies should be included in the district's technology plan. The District should identify staff members who have the authority to enter into contracts. This is especially critical due to "Click-Wrap" software that is acquired simply by clicking "accept" to a provider's terms of service. With click-wrap agreements, the act of accepting the TOS creates a contract between the provider and the district. Not only creating, but also enforcing internal controls is necessary to prevent inadvertent or ill-considered contractual arrangements with online vendors.

Use a written contract.

In light of the foregoing, having a well-drafted agreement is the best way to protect your district and your students. When reviewing, negotiating and drafting agreements with online providers, the districts should consider:

Information Utilization, Retention, Destruction and Disclosure Language

As the Google case has taught us, sometimes vendors collect information for purposes unrelated to education. Thus, it is imperative to understand the differing online models and specifically delineate the purposes for which a provider may use student information. Sometimes, providers collect and maintain student information in a "cloud" environment on the district's behalf. Under these circumstances an agreement should specify how the district is maintaining control over that information and under what

circumstances the provider may share student information. The contract should specify that they may only share data in a manner consistent with FERPA.

In other circumstances, students interact with an online application. To set up accounts districts often share "directory information." Directory information is essentially the student's name, address and phone number. Accordingly, an agreement must specify procedures for the provider to de-identify student information before they may retain it. Also, many vendor contracts are specific to "students." However, they do not address what happens to their information when they are no longer students. Therefore, it is important to include data archiving and destruction requirements to protect information of students who have either graduated, or reside in the provider's database after the contract has lapsed.

Information Collection and Protection Language

Vendor agreements are generally vague or divert liability for failure to maintain student information privacy. Therefore, when appropriate, specify what information the provider will collect and whether that information belongs to the school district or the provider. Define each party's responsibilities with regard to audits and data breach.

Parental Information Access Language

Parents and eligible students have the right to access student information. Therefore, an agreement may need to specify the process for how the school, district and/or parents will be permitted data access. This is vital if the online provider will be creating a new educational record that they maintain for the district. It is prudent for the district to receive requests and forward them to the vendor. This will help to avoid miscommunications and create a district request record.

Term, Termination and Amendment Language

Many technology agreements have automatic renewal provisions which allow the vendors to amend their terms without district consent. Accordingly, an agreement should establish a termination date and procedures for the modification. Amendments and modifications should be in writing and by mutual consent of the parties. Furthermore, the agreement should be clear about the parties' respective responsibilities upon termination, particularly regarding disposition of student information maintained by the provider.

Indemnification Language

Districts can be held liable for a vendor's failure to comply with state or federal laws. Accordingly, districts should demand language that indemnifies the district in this eventuality. Clarify what constitutes potential liabilities, such as a FERPA, PPRA and COPPA violations and that the provider will assume the legal defense if the district gets sued under these, or related, causes of action.

Training, Maintenance and Support Language

Technology providers sell training, maintenance and support to new users. However, it is unclear as to the actual services they provide. Make express how, where, when, and how much training staff will receive. Furthermore, the contract should define when technological support is available and how it will be provided (i.e., in person, email, telephone). Finally, it is important to specify how quickly support will be provided. When an application or program fails it must be restored quickly. Be leery of warranty language that does not guarantee performance ostensibly based on potholes in the "information superhighway." Draft the contracts as though something will go wrong.

Annual notifications

Parental notification is the focus of federal student privacy statutes: FERPA, PPRA and COPPA. Therefore, it is important to be candid with parents and students about how the school collects, shares, protects or uses student data. FERPA requires that districts issue an annual notification to parents regarding their rights (see 34 CFR §99.7). These annual notifications should include effective notice of PPRA and COPPA rights. Beyond these legally required notifications, the technology plan should include periodic parent notifications that explain with whom student data is shared, and post district policies on outsourcing online educational services. If parents are notified and understand their rights they are more likely to help protect student privacy, and less likely to blame the district for privacy violations.

Conclusion

Google has suspended its Google Apps for Education data mining. But dynamic tension between profit motive and privacy remains. There can be a great synergy between technology and education. However, for better or for worse human nature will remain the same — and very few human acts have singular motivation.

That is why all parties must do their jobs. Technology companies and online services are invaluable, but they do not work for free. Schools are trying to find tools to prepare students for the global computer-based economy. However, privacy should be an overriding concern. Information that was once stuffed in a file cabinet now can follow a student for life. A test or assessment that was once thrown in a dumpster can now span the globe in seconds. Districts must be vigilant to draft policies, contracts, and notifications that protect both students and districts at the same time.

—By Gregory J. Rolen, Haight Brown & Bonesteel LLP

Gregory Rolen is a partner in Haight's San Francisco office.