DA District Administration

Professional Opinion

Electronic privacy: Do schools have a role to play?

Changing technologies—and lax regulations—require extra steps to protect information

By:

Christopher J. Librandi

District Administration, March 2014

Christopher J. Librandi is an Connecticut-based attorney who practices business law, including information technology.

The age of textbooks and filing cabinets is coming to an end. Smart phones, tablets and cloud storage are the tools of the day.

Most students probably have their own devices by the time they reach middle school and most school districts use cloud services for record retention and data analysis.

Undoubtedly, these new technologies bring enormous benefits for administrators, students and teachers alike, but they come with risks, particularly to privacy and information security. And we are all too often in the dark when it comes to these risks.

A recent investigation by the Federal Trade Commission found that nearly 60 percent of all mobile applications transmit a user's personal information back to the app developer, an advertising network or another third party—and that this data is most used for targeted advertising. At the same time, only 20 percent of apps disclose their information collection practices to users.

Another study, by the Center on Law and Information Policy at Fordham Law School, found that schools are routinely handing over troves of student information to cloud service providers but that the schools have little knowledge of how the information will be used.

Law? What law?

There are some laws in place to address these privacy risks, but they are by no means a panacea.

The Children's Online Privacy Protection Act (COPPA) requires that online services that are directed at children under 13 or that knowingly collect personal information from children under 13 to disclose their information collection practices clearly and conspicuously.

They must also obtain parental consent before collecting personal information from children. As the statistics just cited indicate, this law is routinely ignored by app developers and website operators.

Meanwhile, the Family Educational Rights and Privacy Act (FERPA) aims to protect student data and information from improper use and disclosure. Like COPPA, this law is regularly overlooked or ignored by schools and their vendors.

In the past couple of years, state and federal agencies have made some efforts to ratchet up enforcement of these laws, but the electronic marketplace is large, fluid and exceedingly difficult for authorities to police. This is where schools can play an important role, stepping in to help fill that significant gap between law and reality.

Forewarned is forearmed

A valuable first step would be to conduct an assembly for students, faculty and parents, providing an overview of the privacy challenges facing the school community. For example, are parents and students aware that many apps employ geo-location tracking of the user?

Tracking is ostensibly used as a means of delivering advertising that is geographically relevant to the user (e.g., promoting a local store), but there are obvious risks inherent in unknown parties following the movements of students.

The goal of the assembly would be to arm teachers, students and parents with a basic understanding of when this kind of tracking is permissible under law; what parents should be looking out for in the apps their children download; and strategies for finding certifiably safe apps.

As a second crucial step, schools should look closely at their vendor contracts to understand what information they are handing over and how the vendor plans to use the information. Has anyone read the vendor's terms and conditions? Do they say anything about use of student information for marketing purposes?

These issues are especially important when dealing with software vendors and cloud service providers. Administrators should be demanding, at a minimum, that their vendors comply with COPPA, FERPA and other privacy protection laws.

Because privacy threats are evolving rapidly, administrators must periodically review changes in the types of technologies their schools employ, the vendors they use, and privacy protection laws affecting them. Ideally, administrators and faculty would receive periodic training to stay abreast of these changes so they can remain valuable resources to parents and students.

Unfortunately, there is no silver bullet against privacy threats in this electronic age, and schools should never over-promise on the protections they can deliver and the awareness they can cultivate.

Nonetheless, administrators are in a position to help faculty, students and parents navigate this increasingly murky landscape, and society as a whole would be well served by savvier, more vigilant school communities.

Christopher J. Librandi is an attorney with the Westport-based law firm Levett Rockwood, P.C., where he practices business law, including information technology. He can be reached at www.levettrockwood.com.