UIC John Marshall Journal of Information Technology & Privacy Law

Volume 30 | Issue 3

Article 3

Summer 2014

Cloud Computing, Regulatory Compliance, and Student Privacy: A Guide for School Administrators and Legal Counsel, 30 J. Marshall J. Info. Tech. & Privacy L. 511 (2014)

Steve Mutkoski

CLOUD COMPUTING, REGULATORY COMPLIANCE, AND STUDENT PRIVACY: A GUIDE FOR SCHOOL ADMINISTRATORS AND LEGAL COUNSEL*

STEVE MUTKOSKI**

EXECUTIVE SUMMARY

Rapid change in the technology landscape has resulted in the introduction of a range of new technologies into the classroom. But unlike the past use of technology in schools, many of these new products and services introduce two new dynamics that school counsel (and the teachers and administrators they support) need to understand fully. First, many of these new products and services are run "in the cloud" by a third party service provider as opposed to on servers operated by the school's information technology (IT) staff. This third party operation and control can raise important new regulatory compliance issues, including data protection and data privacy issues, as the school and student data will be handled by a third party. Second, increasingly these products and services are available without monetary payment for teachers to deploy directly in their classrooms. This means that the products or services often will not go through a more formal procurement process where regulatory compliance and other similar issues would be evaluated.

These new cloud products and services are being widely adopted by schools across the country because they lower school costs, increase productivity, and maximize innovation and efficiency. With a renewed

[*] This Article is based on a paper presented at the Council of School Attorneys National School Law Meeting, October 10-12, 2013.

[**] Director of Public Policy for Worldwide Public Sector, Microsoft Corporation (Steve.Mutkoski@microsoft.com).

partnership between a school's counsel, teachers, school administrators, and school IT staff, those benefits can be reaped without sidestepping important regulatory obligations, such as student privacy. This Article claims to assist these stakeholders in building a better partnership by:

- Explaining the concept of cloud computing and how it is being used in schools;
- Highlighting the regulatory issues raised by new technologies (with a focus on data protection and data privacy issues);
- Offering guidance to school districts who wish to create policies that include mechanisms for legal review prior to deployment of such technologies;
- Providing insight to counsel who are faced with these issues, including a review of applicable law (the Family Educational Rights and Privacy Act and Children's Online Privacy Protection Act in particular) and guidance for negotiating cloud services agreements; and
- Highlighting several emerging developments in both the regulatory and legislative landscape that school decision makers will need to watch for as they chart a course forward.

I. CLOUD COMPUTING IN K-12 EDUCATION

A. WHAT IS CLOUD COMPUTING?

At some point in your career, you (or your IT department) may have experienced the hassle of having to install, maintain, and upgrade different computer applications, such as email and word processing programs, on your computer. This model of computing required significant administrative resources and sometimes delayed the use of new applications as a user waited for upgrades to be deployed across the school or the school district. In recent years, however, advances in technology have ushered in a new era of computing, where many applications are installed, maintained, and upgraded remotely "in the cloud." This means that *instead of storing all data locally on a specific computer, teachers and students can log into their cloud services and access their documents and communications anywhere from almost any device*.[1] To enable this "anytime, anywhere" access, the computer applications (and often lots of data too) are moved from the school's computers to "cloud-based" servers that are operated and maintained by a third-party cloud service provider. As one clever writer explained, it is often easier to understand what cloud computing is by stating what it is not: "[w]hat

[1] Matthew Lynch, *Cloud Computing and K-12 Classrooms*, EDUC. WEEK (Oct. 11, 2013), http://blogs.edweek.org/edweek/education_futures/2013/10/cloud_computing_and_k-12_ classrooms.html.

cloud computing is not about is your hard drive" and "[t]he cloud is also not about having a dedicated hardware server in residence."[2] Most articles on cloud computing will reference one or more acronyms such as IaaS, SaaS and PaaS. Those acronyms are the different "service models" for cloud computing.[3]

Infrastructure as a Service (IaaS) can best be thought of as remote computing capacity (including storage, hardware, servers and networking components) that can be scaled up or down as a particular customer needs more capacity.[4] A key component of the IaaS model is that the customer pays only for the computing capacity that it needs.[5] Many business find that they can deploy services more efficiently and cost effectively with IaaS cloud than they could by maintaining the computing capacity on site. Companies such as Amazon, Microsoft and Google offer IaaS cloud computing.[6]

Software as a Service (SaaS) is akin to what we previously called Application Service Providers or software applications that were delivered as a service over a network.[7] As bandwidth and other technologies have improved in recent years, it has become possible for vendors to deliver an increasing range of applications as services, as opposed to having them run locally on the user's computer.[8] There are a large number of companies providing SaaS offerings, including Salesforce (CRM), Microsoft (Office 365), Google (Google Apps) and Adobe (Creative Suite).[9]

Platform as a Service (PaaS) involves the provision of a complete development environment on which developers can program, debug and execute their new applications.[10] As such, PaaS is primarily aimed at customers who have in-house software developers.[11]

[2] Eric Griffith, *What Is Cloud Computing?*, PC MAG. (Mar. 13, 2013), http://www.pcmag.com/article2/0,2817,2372163,00.asp.

[3] *Cloud Computing: Service Models*, WIKIPEDIA, http://en.wikipedia.org/wiki/Cloud_computing#Service_models (last visited May 22, 2014).

[4] GRACE LEWIS, SOFTWARE ENG'G INST., CARNEGIE MELLON UNIV., BASICS ABOUT CLOUD COMPUTING 1, 2 (2010), *available at* http://www.sei.cmu.edu/library/assets/whitepapers/Cloudcomputingbasics.pdf.

[5] *Id.* at 4.

[6] *Id.* at 3.

[7] Charles McLellan, *SaaS: Pros, Cons, and Leading Vendors*, ZDNET (Mar. 4, 2013), http://www.zdnet.com/saas-pros-cons-and-leading-vendors-7000011500/.

[8] Denise Dubie, *The Top Five SaaS Risks and How to Mitigate Them*, CLOUD COMPUTING J. (May 17, 2013), http://cloudcomputing.sys-con.com/node/2659458.

[9] McLellan, *supra* note 7.

[10] Deniz Kuypers, *PaaS Explained: Benefits & Key Players*, BUSINESS-SOFTWARE.COM (July 12, 2012), http://www.business-software.com/blog/platform-as-a-service-explained-benefits-key-players/.

[11] *Id.*

Other terms that are pertinent to a discussion on cloud computing are public, private, community and hybrid. The concept of "public cloud" is an important one and refers to a (often very large) data center where the workloads of many different customers are run together.[12] The data and workloads of different customers are merely "logically separated" (meaning that a cloud operating system keeps them separate), so the public cloud operator is able to get a high utilization rate across the data center as a whole by taking on a diverse set of customers who have workloads that peak at different times of the day, week, month or year.[13] The higher utilization rate and various other economies of scale in turn allow the operator to charge customers less than it would cost the customer to operate its own servers on site.[14]

The term "private cloud" is used to refer to instances where a single customer wants "physical separation" of its data and computing workloads (often for security purposes).[15] Many people are opposed to using the term because they suggest that such physically isolated servers are just regular old data centers. Regardless of whether the criticism of the term is accurate, it is true that private cloud results in loss of many of the efficiencies and economies of scale that are driving the growth of public cloud, since the cloud provider cannot aggregate multiple customers across that data center.[16]

"Community cloud" is a new concept that attempts to combine some of the cost savings of public cloud with some of the security benefits of private cloud. It involves the sharing of what is effectively a private cloud between several organizations or agencies.[17] This approach has proven popular with the U.S. government, who has purchased such community cloud capacity from companies such as Amazon,[18] Microsoft,[19] and IBM.[20]

[12] *Public Cloud Computing*, GARTNER, http://www.gartner.com/it-glossary/public-cloud-computing/ (last visited June 6, 2014).

[13] Gopan Joshi, *Is My Public Cloud Too Public? Part 3*, CLOUD TWEAKS (May 18, 2012), http://cloudtweaks.com/2012/05/is-my-public-cloud-too-public-part-3/.

[14] ROLF HARMS & MICHAEL YAMARTINO, MICROSOFT, THE ECONOMICS OF THE CLOUD 1, 2-3 (Nov. 2010), *available at* http://www.microsoft.com/en-us/news/presskits/cloud/docs/the-economics-of-the-cloud.pdf.

[15] *Id.* at 13.

[16] *Id.* at 15.

[17] Brandon Butler, *Community Cloud Services: The Next Big Thing*, PC WORLD (Mar. 1, 2012), http://www.pcworld.com/article/251113/community_cloud_services_the_next_big_thing_.html.

[18] *US Federal Government*, AMAZON, http://aws.amazon.com/federal/ (last visited May 22, 2014).

[19] Kirk Koenigsbauer**,** *Announcing Office 365 for Government: a US Government Community Cloud*, MICROSOFT ON GOV'T BLOG (May 30, 2012), http://www.microsoft.com/government/enus/federal/futurefed/pages/details.aspx?Announci

The term "Hybrid cloud" is a mixture of the previously mentioned models and often includes some on-premises computing.[21] A hybrid cloud allows the customer to keep reaping the benefits of cost savings with cloud computing, but also gain security and other control benefits from having on premises computing.[22]

B. EXAMPLES OF CLOUD COMPUTING IN EDUCATION

There are a host of different applications of cloud computing to the school setting, starting with basic productivity tools like email, word processing and spreadsheets.[23] Schools are increasingly expanding into new areas including infrastructure to provide online classes, tools that track and measure student progress and a whole range of learning-based applications.[24] Using the taxonomy above, the majority of cloud applications directed at the education market today are SaaS cloud services that operate in the "public" cloud.[25] In the productivity tools space, Microsoft[26] and Google[27] have offerings that provide students, staff and teachers with traditional email and other productivity tools (like word processing), all of which are cloud-based. Beyond that, companies such as Nulu[28] provide cloud-based language education tools, CourseSmart[29] provides online textbooks, Uzinggo[30] provides online

ng-Office-365-for-Government:-a-US-Government-Community-Cloud&blogid=156.

[20] *Federal Community Cloud for Federal Organizations*, IBM, http://www-304.ibm.com/industries/publicsector/us/en/contentemplate1/!!/xmlid=207581 (last visited May 22, 2014).

[21] Sharon Wagner, *Your Hybrid Cloud: Not If, but When, and How*, VENTURE BEAT (May 27, 2014), http://venturebeat.com/2014/05/27/your-hybrid-cloud-not-if-but-when-and-how/.

[22] *Id.*

[23] *See* JOEL REIDENBERG, N. CAMERON RUSSEL, JORDAN KOVNOT, THOMAS NORTON, RYAN CLOUTIER, & DANIELA ALVARADO, PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS 1, 17-18 (2013), *available at* http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip [hereinafter PRIVACY AND CLOUD COMPUTING IN SCHOOLS].

[24] *Id.* (discussing a taxonomy and cataloging of the wide range of cloud computing services in use in schools today).

[25] *Id.*

[26] *Office 365 Education*, MICROSOFT, http://office.microsoft.com/en-us/academic/ (last visited May 22, 2014).

[27] *Apps for Education,* GOOGLE, *http*://www.google.com/enterprise/apps/education/ (last visited May 22, 2014).

[28] NULU, http://www.nulu.com/ (last visited May 22, 2014).

[29] COURSESMART, http://www.coursesmart.com/ (last visited May 22, 2014).

[30] UZINGGO: GET MATH AND SCIENCE!, http://www.uzinggo.com/ (last visited May 22, 2014).

tutoring, and Edmodo[31] provides a range of cloud-based teaching tools. There are even indications that social networking tools like Facebook[32] and Twitter[33] are used in schools. And the expectation is that this is only the beginning; with significant amounts of venture capital funding for "ed tech," we are likely to see an even greater variety of technology aimed at the classroom.[34]

C. CONSUMERIZATION OF IT (COIT) AND BRING YOUR OWN DEVICE (BYOD)

The trends of "Consumerization of IT" and "Bring Your Own Device" are changing the way that IT is deployed in many businesses and enterprises around the world, and schools are no exception. COIT refers to an important dynamic in the technology world that increasingly new technologies are emerging first in the consumer market and then migrating into the business and enterprise market.[35] This dynamic is reinforced by the fact that people want to use the same technologies at work as they do at home, because they are likely to feel more productive with those technologies. While many people point to the Apple iPad and iPhone as the primary examples of this trend, reinforced by "BYOD" policies that allow employees to connect personal devices to corporate systems, the reality is that it extends far beyond hardware and increasingly into applications and services. Increased user familiarity with the devices and tools that they use at home is definitely a benefit, but there are risks and challenges with these devices, applications and services coming into a workplace.[36]

BYOD policies often require that personal devices include management software or minimum security policies before they are

[31] *About*, EDMODO, http://www.edmodo.com/about (last visited May 22, 2014).

[32] *The Facebook Guide for Teachers*, ELEARNING INDUS. (July 28, 2013), http://elearningindustry.com/the-facebook-guide-for-teachers.

[33] *Twitter in the Classroom*, POWERFUL LEARNING PRACTICE (Apr. 27, 2012), http://plpnetwork.com/2012/04/27/twitter-in-the-classroom/; Samantha Miller, *50 Ways to Use Twitter in the Classroom*, TEACHHUB.COM, http://www.teachhub.com/50-ways-use-twitter-classroom (last visited May 22, 2014).

[34] Dennis Carter, *Venture Capital Funding for Ed Tech at 'Unprecedented' Levels, Expected to Rise,* ECAMPUS NEWS (July 10, 2012), http://www.ecampusnews.com/technologies/venture-capital-funding-for-ed-tech-at-unprecedented-levels-expected-to-rise/.

[35] *Consumerization*, WIKIPEDIA, http://en.wikipedia.org/wiki/Consumerization (last visited May 22, 2014).

[36] *See* Pete Goldin, *Consumerization of IT Still a Threat to Corporate IT Security*, DATA & STORAGE MGMT REP. (July 8, 2013), http://datastoragereport.com/consumerization-of-it-still-a-threat-to-corporate-it-security.

connected to a workplace network to reduce security risks.[37] But as the consumerization trend has moved beyond just devices to include applications and services, workplaces need new internal controls and policies that address not just security risks, but also regulatory risks associated with storage of non-public data on servers operated by third party service providers. Many industries have regulatory requirements that govern how and where their data can be stored and who can access or use that data (the education sector included).[38] One of the regulatory challenges with employees "bringing their own" applications and services, is that those applications and services are governed by terms of service that require the employee to accept the terms prior to use, and once accepted, may result in non-public data being placed in the hands of third parties under terms that are at odds with the employer's regulatory obligations.[39] And often clicking "I agree" or "I accept" is all that is required, since most online services and applications are accompanied by such "clickwrap" or "clickthrough" agreements.[40] The important takeaway is that schools should consider implementing policies that require teachers to get approval of terms of service for such services as per normal procurement review guidelines. Teachers should understand that they may not bind the school (or students) to the provider's terms of service without formal review.

In the school setting, this might play out as follows: A teacher finds an interesting new cloud service that is available for no cost and that she would like to use with her students. So she signs up herself, creates accounts for her students, and begins using the service in her classroom. In the process of registering for and using the service, the operator of the service has access to a range of information about the students, including their names, their web browsing history, and even the content of the assignments which they are writing and storing on the service.

[37] Tom Kemp, *Consumerization of IT Raises New Security Challenges,* FORBES (Oct. 5, 2011), http://www.forbes.com/sites/tomkemp/2011/10/05/consumerization-of-it-raises-new-security-challenges/.

[38] *See, e.g.*, Grant Elliott, *The Pros and Cons of the Cloud*, GOV'T HEALTH IT (May 27, 2014), http://www.govhealthit.com/blog/pros-and-cons-cloud#.U5KDiPmwJgl (highlighting data privacy and security requirements for electronic protected health information imposed by HIPAA); Thomas Trappler, *Cloud Computing: You Can't Outsource your Compliance Obligations*, COMPUTER WORLD (May 21, 2012), http://www.computerworld.com/s/article/9227338/Cloud_computing_You_can_t_outsource_your_compliance_obligations?pageNumber=1 (discussing FERPA regulatory requirements for the education sector).

[39] Jeff Clark, *Is BYOD as Good as It Seems*, DATA CTR. J. (June 4, 2013), http://www.datacenterjournal.com/it/byod-good/.

[40] *Clickwrap*, WIKIPEDIA, http://en.wikipedia.org/wiki/Clickwrap (last visited May 22, 2014).

D. AD-FUNDED "FREE" SERVICES

As one noted legal and policy expert highlighted in the context of discussing contractual considerations that need to be addressed by educational institutions in cloud services contracts:

> Allegedly "free" services require the entity to ask the question of "what is in it for the vendor?" For many web vendors, their business model revolves primarily around advertising; marketing plays a supporting role.[41]

For some free services, vendors will seek to make money not from the sale of the service itself, but from mining and scanning user data to create advertising and marketing profiles.[42] These so-called "ad-supported" businesses have proliferated in the world of consumer services, and as schools and teachers have experimented with new technologies, some of the services offered by these ad-supported businesses have found their way into schools.[43] And while these services are often advertised as "free" or "low cost," they have hidden costs associated with the use (or misuse) of student data through data mining technology.[44] That process involves the use of tools which "allow the provider to trawl through customer information, either individually or on a collective basis."[45] As one education technology expert explained: "If you're able to get a whole university's email on your system, there's a wealth of information to mine."[46] Use of these services can raise both regulatory issues (can student and faculty data be used in this manner consistent with FERPA and/or COPPA?) as well as more normative issues (are parents and students aware that data will be used in this manner and, regulatory issues aside, are they comfortable with those practices?).

[41] Tracy Mitrano, *Legal and Policy Contractual Considerations*, CORNELL U., http://www.it.cornell.edu/policies/cloud/paper/legal.cfm (last visited May 22, 2014).

[42] *See* Daniel Solove & Paul Schwartz, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1850-53 (2011) (generally discussing the ways in which user activity and data can be collected and used to target advertising to the user).

[43] Josh Grolin, *'Free' Cloud Services Erode Student Privacy*, BOSTON GLOBE (Apr. 21, 2014), http://www.bostonglobe.com/opinion/2014/04/21/free-cloud-services-erode-student-privacy/4SMdpd1NXrGDVzgdwEptyJ/story.html.

[44] Christopher Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 626-28 (2014).

[45] Chris Reed, *Information 'Ownership' in the Cloud*, QUEEN MARY SCH. L. & LEGAL STUD. RES. PAPER 1, 45 (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461.

[46] *See* John Ross, *Cloud Giants Capture them Young,* AUSTRALIAN (Apr. 8, 2013, 12:00 AM), http://www.theaustralian.com.au/higher-education/cloud-giants-capture-them-young/story-e6frgcjx-1226613374010).

II. DATA PROTECTION AND DATA PRIVACY ISSUES WITH CLOUD COMPUTING IN EDUCATION

While cloud computing presents a great opportunity for teachers and schools, it also creates data protection and data privacy issues by placing a very large amount of student, teacher, and institution data in the hands of a third party service provider. Consequently, it is critical that teachers, school administrators, and school counsel take steps to ensure that the cloud services that are used in the classroom and the administrative offices comply with all applicable laws and otherwise protect student, teacher, and institution data from improper use. There are at least three sources that are useful to guide these stakeholders as they establish policies on the deployment and use of cloud services in the classroom: (1) FERPA, (2) COPPA and (3) norms and attitudes related to student privacy.

A. THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)[47]

FERPA protects the privacy of student data contained in a range of written and electronic records – generally, anything that is considered "personally identifiable information" in an "education record," including e-mails and other communications or documents created by students, teachers and administrators.[48] School policies related to the deployment of new technologies should provide guidance for obtaining review of the FERPA implications of the specific technology. The term "education record" is broadly defined to mean "records, files, documents, and other materials" that: (1) "contain information directly related to a student"; and (2) "are maintained by an educational agency or institution or by a person acting for such agency or institution."[49] While not every email or other electronic document created by a teacher or school administrator in the school setting may be an education record, it is clear many have content that "qualifies as a student record."[50]

[47] *See* 20 U.S.C. § 1232g (2013).

[48] Note that under FERPA, institutions may choose to disclose certain information (which would otherwise be protected under FERPA) as "directory information." As a result, it is technically only non-directory PII contained in a student record that is restricted under FERPA, assuming that parents have not opted out of disclosure of directory information. PRIVACY AND CLOUD COMPUTING IN SCHOOLS, *supra* note 23, at 4-5.

[49] U.S. DEP'T OF EDUC. PRIVACY TECHNICAL ASSISTANCE CTR., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES 1, 2 (Feb. 2014), *available at* http://blogs.edweek.org/edweek/DigitalEducation/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf; *see* 34 C.F.R. § 99.3 (2012) (definition of "education record").

[50] Joseph C. Storch & Seth F. Gilbertson, *Cloud Contracting: Outsourcing e-mail at Your University*, NACUA NOTES (Dec. 16, 2009),

Additionally, FERPA's protections extend only to "PII" (or Personally Identifiable Information in an education record).[51] The term PII is defined to include not only specific identifiers such as name, address or student number, but also a catchall of "[o]ther information that, alone or in combination, is linked or linkable to a specific student" that would allow someone in the school community "to identify the student with reasonable certainty."[52] It may be difficult to parse through a document and make a clear determination about what is or is not PII, particularly in light of new technologies that allow diverse bits of data to be aggregated to "re-identify" the person whom that data describes.[53]

The U.S. Department of Education (DOE) has issued guidance explaining how FERPA applies when a school uses a cloud service provider to maintain and operate IT services such as cloud-based email services.[54] The DOE's position is that the handling and storage of institution data such as email by a service provider is viewed as a disclosure under FERPA and as such either requires parental consent or an exception from consent if FERPA protected information is included in that communication.[55] The Department's guidance is that institutions may use the so-called "school official" exception for disclosure of education records in such situations, but only if three conditions are met:

> Specifically, the outside party must: 1) perform an institutional service for which the . . . school would otherwise use employees; 2) be under the direct control of the . . . school with respect to the use and maintenance of education records; and 3) be subject to the requirements in § 99.33(a) of the FERPA regulations governing the use and redisclosure of PII from education records.[56]

http://counsel.cua.edu/FERPA/publications/NACUANoteCloudContract.cfm.

[51] U.S. DEP'T OF EDUC. PRIVACY TECHNICAL ASSISTANCE CTR., *supra* note 49, at 2-3.

[52] *Id.*; *see* 34 C.F.R. § 99.3 (definition of "personally identifiable information").

[53] "The same problem exists for the distinction between PII and non-PII. The line between PII and non-PII is not fixed, but depends upon technology. Thus, today's non-PII might be tomorrow's PII." Solove & Schwartz, *supra* note 42.

[54] *See generally Frequently Asked Questions—Cloud Computing,* PRIV. TECH. ASSISTANCE CTR. (June 2012), http://ptac.ed.gov/sites/default/files/cloud-computing.pdf; *see generally Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, PRIV. TECH. ASSISTANCE CTR. (Feb. 2014), http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20(February%202014).pdf .

[55] U.S. DEP'T OF EDUC. PRIVACY TECHNICAL ASSISTANCE CTR., *supra* note 49, at 3-4.

[56] *Frequently Asked Questions—Cloud Computing*, *supra* note 54, at 2.

What does this mean for school staff and boards examining cloud platforms? In broad terms, it means that there are some complicated legal and regulatory issues that should be reviewed with legal counsel. The following are some of the more specific FERPA issues raised by modern cloud based technologies in the classroom.

- *What is an Education Record under FERPA?:* What information does the cloud application or service put in the hands of a third party service provider and is any of that information something that might be considered an "education record?" This is a challenging inquiry since technology is still evolving. Clearly things like email can be education records, but how about teacher notes about performance that are stored in an online service that tracks student progress? The reality is that the concept of an "education record" was developed decades ago when much of our current technology did not exist. In its most recent guidance, the DOE has highlighted the challenging nature of this inquiry, posing the question "Is Student Information Used in Online Educational Services Protected by FERPA?" and responding "It depends."[57] We can see from the DOE guidance that many new technologies are likely to result in the storage or transmission of information that will be considered an education record under FERPA.[58] It may be prudent for school policy to include a presumption that all data created by students, teachers, and staff be considered education records for purposes of directing third party technology providers as to how they should handle the data, how they can use it, and with whom they can share it.
- *What is PII?:* Similarly, what portions of an education record should be considered PII is a challenging and context specific inquiry. Expert commentary has suggested the concept of PII is no longer as meaningful as it once was and indeed that customers and online service providers may have very different conceptions of what is or is not PII.[59] School districts may want to preclude third party service providers from making determinations about what elements of an education record are or are not PII, by ensuring that the use of all student and institution data by the vendor is restricted.
- *Meta data and de-identification:* The DOE's most recent guidance does refer to "[m]etadata that have been stripped of all direct and indirect identifiers" and notes that such information "are not considered protected information under FERPA because they are not PII."[60]

[57] *Protecting Student Privacy*, *supra* note 54, at 2.

[58] *Id.* at 2-3.

[59] Solove & Schwartz, *supra* note 42, at 1818 (noting that "companies have also tried to short-circuit the discussion of legal reforms through the simple argument that they do not collect PII").

[60] *Protecting Student Privacy*, *supra* note 54, at 3.

Of course when it comes to "de-identification" of data or metadata, the devil is in the details and we are increasingly learning in other contexts that metadata may be far more intrusive than previously thought.[61] It is also important to note that FERPA's definition of PII includes a catch-all which refers to "[o]ther information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty."[62] As one education industry group pointed out when discussing FERPA's PII catch all, "[t]he 'de-identification' of data, including metadata, raises some highly challenging issues and you will probably want to consult your School's counsel, as well as an expert in data issues before you undertake to de-identify data or allow a service provider to do so."[63] As a result, you will also want to include terms in your agreements with service providers that require full disclosure of any plans to de-identify institution or student data, including an opportunity to review and approve the service provider's de-identification methodology.

- *Who is a "school official" and what restrictions must be placed on their access to and use of education records protected by FERPA?*: The school official requirement that the service provider be under the "direct control"[64] of the institution strongly suggests that important decisions about the handling and use of FERPA protected data, including what institution or student data is actually subject to FERPA, will be made by the institution. Direct control also anticipates that the institution will dictate how the service provider is authorized to use institution data and how it may not use the data. Additionally, the school official must use the FERPA-protected information "only for the purposes for which the disclosure was made."[65] Where the disclosure of FERPA-protected information is made in connection with the provision of a cloud computing service, the service provider may only use the information for the purposes of providing that contracted service and not for other collateral purposes.[66] The DOE's most recent guidance includes several examples that address one current hot button issue—use of

[61] *Snowden, Greenwald: Metadata Monitoring Worse than Eavesdropping*, NEWS MAX (Apr. 5, 2014), http://www.newsmax.com/Newsfront/AmnestyInternational-chicago-meeting-surveillance/2014/04/05/id/563875/.

[62] 34 C.F.R. 99.3 (2012).

[63] *Protecting Privacy in Connected Learning Toolkit*, COSN (Mar. 2014), http://cosn.org/protecting-student-privacy-toolkit.

[64] 34 C.F.R. § 99.31(a)(1)(i)(B)(2) (2012).

[65] *Id.* at § 99.33(a).

[66] *Protecting Student Privacy*, *supra* note 54, at 4-5.

student data for targeted advertising purposes.[67] Examples 2 and 4 in the U.S. Department of Education's most recent guidance make it clear that FERPA protected information may not be used by a service provider to "target ads to individual students . . . because using the data for these purposes was not authorized by the district and does not constitute a legitimate educational interest."[68]

A range of K-12 and higher education groups have released or are working on new materials related to the application of FERPA in the school or university setting, including the previously mentioned toolkit from CoSN,[69] materials from the Harvard Berkman Center[70] and materials from the National School Boards Association.[71]

B. THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)

COPPA is a federal law that regulates the online collection, use, and disclosure of personal information from children under the age of thirteen.[72] At a high level, the purpose of COPPA is to protect the privacy and safety of children and to limit how operators of online services market to children.[73] COPPA applies to operators of commercial websites and online services directed at children under the age of thirteen or operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under thirteen.[74] Most importantly, COPPA requires that such operators obtain parental consent before undertaking such activities.[75]

The Federal Trade Commission (FTC) enforces COPPA and has issued guidance explaining how COPPA applies when a school contracts

[67] *Id.* at 5-7.

[68] *Id.*

[69] *Protecting Privacy in Connected Learning Toolkit*, *supra* note 63.

[70] *Berkman Center for Internet & Society Student Privacy Initiative*, HARVARD U., http://cyber.law.harvard.edu/research/studentprivacy (last visited May 22, 2014).

[71] *NSBA Previews Student Data Privacy in the Cloud Policy Guide*, NSBA (Apr. 6, 2014), http://schoolboardnews.nsba.org/2014/04/student-data-cloud/.

[72] *See generally* Children's Online Privacy Protection Rule, 16 C.F.R. Part 312 (2013).

[73] *Id.*

[74] A full discussion of what constitutes "personal information" under COPPA is beyond the scope of this Article, but it is important to highlight that the concept is fairly broad and recent FTC rule revisions have expanded that term to include photos, videos, audio recording, and geolocation data. *See Complying with COPPA: Frequently Asked Questions*, BUREAU OF CONSUMER PROTECTION: BUS. CTR. (Jul. 2013), http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions, [hereinafter *COPPA: F.A.Q.*].

[75] *See id.* (Question H1 "When do I have to get verifiable parental consent?").

with a cloud vendor to provide online services to students.[76] The FTC's guidance on COPPA (a series of Frequently Asked Questions that has been updated over time, including in April and July 2013)[77] now includes four questions and answers related to how COPPA applies in the school setting.[78] While some people initially thought that COPPA didn't apply to most schools (because they are non-commercial), the FTC guidance makes it clear that it is the service provider's activities and use of personal information that are the gauge of whether COPPA will apply. The four current FAQ's make it clear that where operators of commercial services and websites provide those services to schools, COPPA must be considered.[79]

1. Parental Consent under COPPA and the Role of Schools

The first two questions related to COPPA and schools were modified in 2013 and seek to explain the *role that schools may play in obtaining or providing parental consent* where COPPA is brought into play, and more importantly, the circumstances under which an operator may or may not rely on the school as an agent or intermediary for such parental consent. Those questions are:

(a) Can an operator of a website or online service rely upon an educational institution to provide consent to the operator's collection, use, or disclosure of personal information from students?

(b) Under what circumstances can an operator of a website or online service rely upon an educational institution to provide consent?

The commentary in response to these two questions provides several important pieces of guidance to schools and operators of online services on the topic of parental consent. First, the commentary makes clear that the school may provide consent under COPPA on behalf of parents (and the vendor may rely on that consent), under certain circumstances, stating:

> COPPA does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parent's agent in the process of collecting personal information online from students in the school context.[80]

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Complying with COPPA: Frequently Asked Questions: M. COPPA and SCHOOLS*, BUREAU OF CONSUMER PROTECTION: BUS. CTR. (Jul. 2013), http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools [hereinafter *COPPA and SCHOOLS*].

[80] *Id.*

Second, the commentary provides some insight into the circumstances where vendors may rely on schools as the agent or intermediary for parental consent. The commentary highlights the need for schools to understand fully the purpose for which any personal information from students is collected and how it is used or shared by the operator, stating:

> Determining whether the school may provide consent on behalf of a parent, or whether the operator can rely on the school for consent, will depend on the nature of the relationship between the online service and the school or child, and the nature of the collection, use, or sharing of the child's personal information.[81]

Third, the commentary creates a distinction between collection, use, or sharing of a child's personal information "for the use and benefit of the school" and collection, use, or sharing for "*other commercial purpose*."[82] As the commentary highlights, an operator will need to obtain actual parental consent where it "intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school."[83] This requirement can present a particular challenge in an era when service providers may have their own plans for collateral commercial use of user data. Schools will need to examine carefully operator data collection, use and sharing policies prior to deploying those services, or agreeing to act as an agent or intermediary for parental consent, to determine whether the service provider should be obtaining consent directly from parents.

2. Questions to ask Cloud Service Operators

The third of the FTC's Frequently Asked Questions on COPPA and Schools, newly added in 2013, provides some of the questions that schools should be asking operators before allowing an operator's services to be deployed in a school. Most pertinent is:

> Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, does it use the students' personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service?[84]

[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.*

This question addresses a common collateral use of user information: online advertising. It also highlights an important concern of schools: ensuring that operators do not plan to use student personal information for such purposes without actual parental consent.

3. Social Networks and Parental Consent

Another 2013 addition to the FTC's FAQ on COPPA and Schools raises a very challenging issue related to the use of online social networks that allow children to participate with parental consent.[85] The crux of the question is whether a school or teacher can provide that consent in lieu of a parent. The FTC commentary makes it clear that schools should give parents full and accurate disclosure of the ways in which a child's personal information may be collected, used or shared by the operator of such a network prior to giving such consent, by providing:

> [W]here the activities and the associated collection or disclosure of children's personal information will extend beyond school-based activities, the school should carefully consider whether it has effectively notified parents of its intent to allow children to participate in such online activities before giving consent on parents' behalf.[86]

Although this specific FAQ refers to social networks, it likely should be considered by schools in connection with the use and deployment of a broad range of account based tools, applications, or services which might have application both inside and outside of schools.

Although the four COPPA and Schools questions and accompany commentary do not answer all questions or provide complete bright line rules, they do offer thoughtful guidance on the types of questions school decision makers should ask operators. School officials should consult in detail with legal counsel regarding COPAA issues, should explore carefully whether operators plan to make collateral commercial uses of student personal information, and should put special measures in place where that is the case to ensure the operator is obtaining consent directly from parents.

C. DATA PROTECTION NORMS: PRIVACY IS NOT DEAD

While we frequently hear pundits claiming that "privacy is dead," the research work that is being conducted in the fields of child and student privacy suggests otherwise. Surveys from a range of countries

[85] *Id.*
[86] *Id.*

highlight the serious concerns that parents, teachers and school administrators have regarding privacy and the use of online services by students.

A January 2013 Brunswick Insight Survey in the United States revealed that three quarters (75-76%) of parents surveyed expressed disapproval of vendor practices that included capturing personal information, scanning email, and tracking students for marketing or advertising purposes.[87] The survey also reported that ninety-three percent of U.S. adults with children in the first through twelfth grades were "concerned" or "very concerned" about online tracking of students in schools.[88] Approximately eighty-four percent of parents reported wanting to be able to take action against this online tracking.[89] As one privacy expert noted in reviewing the data, "the survey revealed that parents are very concerned about their students' online privacy, especially the tracking of their activities and marketing based on behavioral data."[90] More recent surveys in Australia[91] and the UK[92] identified similar concerns among parents and teachers in those countries. New research Commissioned by San Francisco-based nonprofit group Commmon Sense Media and released in 2014, further highlights the concern that student data is improperly being used for commercial purposes.[93] James Steyer, the CEO of Common Sense Media, summarized the survey data, saying "American families feel by incredible margins that students' personal and private information should not be for sale, period."[94]

[87] *See 2012 National Data Privacy in Schools Survey*, SAFEGOV (Jan. 2013), http://safegov.org/media/43502/brunswick_edu_data_privacy_report_jan_2013.pdf.

[88] *Id.*

[89] *Id.*

[90]. Daniel Solove, *Parental Attitudes about Student Privacy Online,* SAFEGOV (Jan. 8, 2013), http://safegov.org/2013/1/8/parental-attitudes-about-student-privacy-online.

[91] *See generally Australian Parents' Views of Cloud Services and Online Privacy in Schools*, SAFEGOV (May 2013), http://safegov.org/media/49377/safegov-australian-parents-survey.pdf.

[92] *See generally UK School Opinions of Cloud Services and Student Privacy*, SAFEGOV (May 2013), http://safegov.org/media/48269/safegov_ponemon_uk_school_survey.pdf.

[93] *Student Privacy Survey*, COMMON SENSE MEDIA 1, 1 (Jan. 2014), http://cdn2-d7.ec.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf; *see also School Privacy Zone*, COMMON SENSE MEDIA, http://www.commonsensemedia.org/school-privacy-zone (last visited Mar. 18, 2014).

[94] Benjamin Herold, *Americans Worried, Uninformed about Student Data Privacy, Survey Finds,* EDUC. WEEK (Jan. 22, 2014, 12:47 AM), http://blogs.edweek.org/edweek/DigitalEducation/2014/01/american_worried_uninformed_student_data_privacy.html.

Indeed, data protection issues concern parents, a crucial segment of the larger community schools serve. Teachers, administrators and counsel play an important role as gatekeepers for their communities on issues such as protection of student privacy. As one policy expert in higher education explained:

> It is therefore imperative that an institution representing its users must examine its own culture, law, and traditions in the area of information privacy and be prepared to make clear claims regarding what is and is not acceptable behavior on the part of the vendor.[95]

It is clear that local norms about student privacy are an important supplement for school officials to consider in addition to federal laws such as FERPA and COPPA and other applicable state and local laws and regulations.

D. THE EMERGING LEGISLATIVE LANDSCAPE: CALLS FOR NEW LEGAL PROTECTIONS

The 2013-14 legislative session is shaping up to be an active one on the issue of student privacy, both at the state and federal level. As of the writing of this Article, a growing number of state legislatures are considering bills that would restrict how student data can be used by cloud service providers. State Senator Steinberg of California has introduced the Student Online Personal Information Protection Act.[96] This bill would restrict an online service provider to using student information only "for school purpose and for maintaining the integrity of the site, service, or application" and would specifically prohibit use of that information for "any commercial purpose, including, but not limited to, advertising or profiling."[97] Similar bills have been introduced in Virginia,[98] Kentucky,[99] West Virginia,[100] Maryland,[101] Maine,[102]

[95] Mitrano, *supra* note 41.

[96] *See* Natasha Singer, *Scrutiny in California for Software in Schools,* N.Y. TIMES (Feb. 20, 2014), http://www.nytimes.com/2014/02/20/technology/scrutiny-in-california-for-software-in-schools.html?ref=technology&_r=0.

[97] CAL. BUS. & PROF. CODE § 22584 (2014).

[98] Va. Code Ann. § 22.1—289.01 (2014).

[99] S. 89, 10th Gen. Assemb., Reg. Sess. (Ky. 2013). An alternative bill containing student privacy protections was signed into law in Kentucky on April 10, 2014. Joe Arnold, *Beshear Signs Data Protection Bill into Law,* WHAS11.COM (Apr. 10, 2014), http://www.whas11.com/news/politics/Beshear-signs-data-protection-bill-into-law254797181.html ("The General Assembly also agreed to additional language from Republican Senate Bill 89, which protects student information from use by software vendors.").

[100] W. VA. CODE ANN. § 61-14 (2014), *available at* http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=hb4279%20intr.htm&yr=2

Nevada, and Idaho,[103] to name just a few others. In addition, Massachusetts Senator Edward Markey has announced he plans to introduce similar student privacy legislation at the federal level in early 2014, which would include a component restricting the commercial uses which service providers could make of student data.[104] While it is still not clear which of these bills will be enacted into law, the significant legislative in the area of commercial uses of student data suggest that school administrators and counsel should be taking a careful look at how service providers intend to use student data to which they will have access.

III. CLOUD CONTRACTING AND DATA PROTECTION: BEST PRACTICES FOR CONTRACTING

In late 2013, researchers at the Fordham Center for Law and Information Policy released a ground-breaking study on the use of cloud computing in schools and the policy and practices of K-12 institutions aimed at protecting the privacy of student data that was stored in or transmitted across such cloud services.[105] The study highlighted that not only are schools rapidly moving to adopt cloud computing services, but they are doing so in a manner that does not adequately safeguard student privacy interests.[106] The study identifies several key areas where school practices could be improved, but most importantly, it highlights poor vendor contracting practices as one area where better practices would go a long way to improving student privacy protections in the cloud computing era.[107] This section outlines some best practices for school administrators and counsel as they approach contracting for cloud services in the K-12 setting. It also suggests that renewed emphasis on establishment and communication of policy within schools and into classrooms is essential and offers some high level guidance for school administrators and counsel as they craft and implement such policies.

014&sesstype=RS&i=4279.

[101] H.R. 607, 2014 Gen. Assemb., Reg. Sess. (Md. 2014).

[102] ME. REV. STAT. tit. 20-A, § 6006 (2014).

[103] S.B. 1372, 2014 Gen. Assemb., Reg. Sess. (Id. 2014).

[104] Leslie Gallagher Moylan, *"A" for Effort? Senator Markey announces Latest Privacy Legislation aimed at Protecting Student Data*, JDSUPRA BUS. ADVISOR (Jan. 17, 2014), http://www.jdsupra.com/legalnews/a-for-effort-senator-markey-announces-63241/.

[105] PRIVACY AND CLOUD COMPUTING IN SCHOOLS, *supra* note 23.

[106] Natasha Singer, *Schools Use Web Tools, and Data is Seen at Risk,* N.Y. TIMES (Dec. 12, 2013), http://www.nytimes.com/2013/12/13/education/schools-use-web-tools-and-data-is-seen-at-risk.html?ref=natashasinger.

[107] PRIVACY AND CLOUD COMPUTING IN SCHOOLS, *supra* note 23, at 67-69.

A. CLOUD CONTRACTING BEST PRACTICES

K-12 schools, consistent with their mission to safeguard a range of student, staff, and organizational interests, including data privacy interests, should endeavor to include in contracts with cloud service providers limits on how the service provider may use student, staff, and faculty data. While we may perceive cloud services as being akin to a locker that the user secures, in reality these are services where the provider can open the door to the locker.[108] And, in a world of increasingly diversified service providers, there may be reasons that one aspect of a service provider's business may want to open up that locker and use what it finds inside. [109]

Data ownership, confidentiality, data privacy, and data protection rights are critical contract terms in many segments where cloud computing is being deployed, and the education sector is no exception. In the past, many data processing agreements with third party vendors relied heavily on concepts such as data ownership and confidentiality to restrain the vendor from using or disclosing customer data in unintended ways. But as more data is moved to the cloud, and as some service providers are increasingly motivated to access customer data for advertising, marketing, or other collateral commercial purposes, customers need additional protections in their contracts with service providers. As the director of licensing for one large university noted, data ownership is only the starting point:

> With ownership clarified, the next step is to identify the limitations on how the cloud provider may use your data. In most cases, you'll want to limit the provider's use solely to that which is necessary for it to fulfill its obligations under the contract. It is also prudent to specifically exclude the provider from any mining of your data.[110]

[108] Chris Hoofnagle, *The Good, Not so Good, and Long View on Bmail*, BERKELEY BLOG (Mar. 16, 2013), http://blogs.berkeley.edu/2013/03/06/the-good-not-so-good-and-long-view-on-google-mail/.

[109] Lauren Tara LaCapra & Jennifer Saba, *Fed Queries Bloomberg Over Reporters' Access to Client Data*, REUTERS (May 11, 2013, 7:57 PM), http://www.reuters.com/article/2013/05/11/us-bloomberg-data-idUSBRE94A0BF20130511 (reporting an incident in May 2013 involving Bloomberg LP demonstrates the potentially conflicting motivations that can arise within a service provider; according to reports, Bloomberg's media reporters had access to data about customer use of Bloomberg's famed terminals and used them to draw inferences about confidential matters within some of the terminal customers that were reported on in Bloomberg's news division).

[110] Thomas Trappler, *When Your Data's in the Cloud, is it Still Your Data?*, COMPUTER WORLD (Jan. 17, 2012, 9:58 AM), http://www.computerworld.com/s/article/9223479/When_your_data_s_in_the_cloud_is_it_still_your_data.

Clauses addressing data ownership and confidentiality do not necessarily restrict the service provider from making collateral commercial uses of your student and teacher data. Confidentiality provisions are primarily aimed at restricting additional disclosure by a receiving party and so would not necessarily preclude an advertising division of a cloud service provider from using data covered by a confidentiality provision to target advertising to users of the service. Similarly, ownership of data can remain vested with the customer, but absent clear usage restrictions, the service provider may be under the impression that it has rights to use customer data for a range of purposes.

The following are several of the best practices for contracting for educational institutions as they embrace cloud computing:

- *Broadly define "Customer Data:"* Contract provisions should define carefully key terms such as "customer data" to include the broad range of student, teacher, and staff data that is transmitted across or stored in the cloud service. Schools should resist service provider attempts to create narrower definitions. In particular, schools should oppose service provider attempts to restrict only use of customer data that is considered "personal information" or allow free use of "anonymized" or aggregated data; the definition and use limitations imposed on the service provider should extend to all customer data and not merely a subset of it.
- *Carefully restrict Provider use(s) of Customer Data*: The contract should restrict the service provider's use of customer data to only what is required for the service provider to operate and to improve the specific contracted service or services. It should not allow the service provider to use the customer data to operate or improve other services or products that the service provider owns or operates. So if the contracted service is an email service, the provider should use the data only for the operation of that service.
- *Prohibit other uses:* The contract should also expressly prohibit uses of customer data beyond what is required to operate and improve the contracted service or services, and should specifically prohibit use of customer data for advertising or marketing purposes. In particular, contracts should carefully distinguish between (a) the scanning or data mining of user content and metadata for authorized purposes such as malware and spam detection; and (b) scanning or data mining of user content and metadata for prohibited purposes such as user profiling or ad targeting. Contracts should explicitly prohibit any form of data mining or scanning of user content for marketing or ad targeting purposes unless the user has expressly provided informed, unambiguous opt-in consent for such processing.

• *Don't simply accept existing terms:* Standard confidentiality clauses or clauses that state the school owns its data are helpful, but will not by themselves preclude the service provider from scanning school data and using it for collateral commercial purposes. Clauses stating that the service provider will not serve advertisements to the school's teachers, staff, or students are similarly ineffective. Even with ad serving turned off, a service provider can continue to scan school data and use that information for other advertising and marketing purposes.

• *Proactively protect the school from the possibility that a service provider will require ad serving to be turned on in the future*: Schools should not accept contracts or terms of service which include an option to turn ad serving back on, but instead should require cloud service providers to remove all ad-related functionality from their services without otherwise modifying their terms and conditions. Schools should require cloud service providers to pledge that turning on ad serving will never be a condition for renewing an existing contract on favorable pricing terms or for continuing to provide the same service and functionality originally offered to the school.

• *Address FERPA compliance issues:* Because of challenging questions related to what is or is not "PII" in an "education record," it can be a challenging exercise to draft a contract clause that adequately addresses FERPA compliance obligations. One way to secure FERPA compliance with cloud services is to restrict a cloud provider's ability to collect, use, or share any institution data beyond what is necessary to operate and improve the specific contracted service or services. You may also want to use a belt and suspenders approach and specifically call out that other commercial uses of institution data, such as for advertising or marketing purposes, are not permitted under the contract.

• *Address COPPA compliance issues:* To ensure that the school is able to act as an agent or intermediary for parental consent under COPPA, the contract should require that the operator's collection, use, or sharing of a child's information is only for the use and benefit of the school and make clear that the operator is not allowed to collect, use, or share a child's information for any other commercial purpose. If the service provider expresses any intent to make other commercial uses of the student or institution data, you should require the provider to fully disclose all such uses to and obtain express consent from parents, prior to deploying the service.

B. Cloud Computing Services in the Classroom: Establishing District Policy

Whether free or for cost, whether "click thru" or formal agreement, any agreement that a teacher, staff, or administrator enters into that purports to bind the school or school district will need to be vetted by legal staff. Anecdotal evidence suggests that today many teachers are deploying new technologies in their classrooms without any legal review of the terms and conditions that govern the use of these technologies.

Districts should review their current policies and actual practice, but they will likely want to institute policies that cover the following items:

- Legal review of online services terms and conditions prior to use by students;
- Collection, use and sharing of student, teacher or administration data that is stored on or transmitted through a third party cloud service;
- Contractual requirements that ensure FERPA compliance; and
- Contractual language for online services that may be used by students under thirteen, ensuring that the school is able to act as the agent or intermediary for parental consent under COPPA.