IMPACT OF FEDERAL RULES (INCLUDING FERPA) ON CLOUD COMPUTING – REQUIREMENTS FOR COMPLIANCE/ SUGGESTIONS FOR BEST PRACTICES

Presentation by William A. Hornback
August 1, 2014

I. INTRODUCTION

As it appears all educational agencies, to one degree or another, are either moving into or already engaged in cloud computing, there have been significant discussions and concerns raised at all levels about the safety and security of student and other data which is migrating into the cloud.[1]

To better understand the situation, we first note "cloud computing" is a marketing term. Essentially, the term "the cloud" is really just a metaphor for the Internet. The term "in the cloud" refers to several items sold as a service and may include software as a service (SaaS)[2], a platform as a service (PaaS)[3], or infrastructure as a service (IaaS).[4] As the technology and innovation expand, we also see such offerings as desktop as a service (DaaS), backend as a service (BaaS), and IT management as a service (ITMaaS).

For example, a vendor may have large remote servers that host users' software, and more, via the Internet. Users log on to the vendor's network and begin work. Cloud services are offered in public, private, or hybrid networks, with some forms creating additional concerns for the control of confidential information. Google, Amazon, IBM, Oracle Cloud, and Microsoft Azure are just a few of the cloud vendors.

[1]There will be no discussion of the distinctions between various forms of the "cloud" including "public cloud" or "private cloud" or "hybrid cloud" or "community cloud" or partner cloud."

[2]Examples are Google Apps, Adobe Creative Suite, Microsoft Office (365); typically forms of software licensing that outsource the IT burdens related to software management allowing users to access software via an Internet browser.

[3]As where a provider offers use of a network which may include both hardware and software and may be used to host a district's particular application.

[4]Sometimes referred to as hardware as a service (HaaS), it is utilization of provider-owned hardware operating, storing, maintaining district software and data.

Vendors "in the cloud" consistently seek to improve their products and services and often sell data to others. Cloud vendors routinely collect information from users, which is permitted by the disclosure to and user's acceptance of the usage and sharing permissions contained in the "terms of service" (TOS) the user must agree to in order to access or use the product.

Conversely, educational agencies have ongoing and increasing obligations relating to confidential information, particularly student information, at the same time that funding is being reduced, technology is becoming more prevalent in the classroom, and innovation is being offered via online educational products. All of this must remain within the confines of the Family Educational Rights and Privacy Act (FERPA) when student "educational records" are involved. Among the restrictions under FERPA are restrictions on both disclosure and redisclosure of protected information without an express written consent signed by the parent or student over 18 years old.[5] When the data is "in the cloud," this could mean the express written consent from the parents of every pupil.

Whether the district's version of the cloud is simple offsite storage or online educational or instructional tools or more, you will have an obligation to ensure the confidentiality of your educational records and to manage whether and how they are used and/or disclosed to others. This includes any intended uses of the cloud vendor you have chosen. If you have not reviewed the cloud vendor's TOS or other contractual provisions in detail, or agreed to the TOS without review, you may be at risk. This also applies to any "app" downloaded by teachers for use in the classroom, either on their own personal devices or on district computers, iPads, tablets, or smartphones. Each app has its own set of TOS.

II. PERSONALLY IDENTIFIABLE INFORMATION

There are two kinds of educational records, those containing personally identifiable information (PII) and those that do not contain PII. It is essential that there be an understanding of what constitutes PII. "Personally identifiable information" is defined as follows:

"The term includes, but is not limited to—
(a) The student's name;
(b) The name of the student's parent or other family members;
(c) The address of the student or student's family;
(d) A personal identifier, such as the student's social security number, student number, or biometric record;
(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

[5] 34 CFR, Section 99.30(a): "The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31."

(f) Other 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; or
(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates."[6]

"Educational records" are defined as any records directly related to a student that are maintained by an educational agency or by a party acting on its behalf.[7] Educational records that contain PII are protected from disclosure under FERPA and state law.

It is important to note that the definition of PII also includes other information that, alone or in combination, is linked or linkable to a specific student and would allow a reasonable person to identify the student with reasonable certainty, or any information requested by a person who is believed to know the identity of the student to whom the information relates. Thus, small portions of educational records could, in combination, constitute protected PII. This raises the possibility that metadata and other digital data "in the cloud" could, when found in various combinations, identify a student. If it does, an express exception must be utilized before the data is either released by the district or re-released by the cloud vendor.

III. DE-IDENTIFIED RECORDS AND INFORMATION

All educational records bear some protections, for the most part reflecting the need for de-identification of such records prior to their release. This means all PII must be removed. The devil is in the details, as always, since any combination of information, both contained in and outside educational records, that could lead to identification of a student is considered PII under FERPA rules. As such, it would have to be removed before being disclosed unless one of the permitted exceptions applies. The same rules apply to a cloud vendor to whom the information has been or is being released.[8]

There are different tools for de-identification of student data. "Anonymization" results in de-identified student data that lacks a record code needed to link the records, similar to looking

[6]34 CFR, Section 99.3.

[7]34 CFR, Section 99.3.

[8]34 CFR, Section 99.31(b)(1): "An educational agency or institution, or a party that has received education records or information from education records under this part, may release the records or information without the consent required by §99.30 after the removal of all personally identifiable information provided that the educational agency or institution or other party has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information."

at a record not bearing the student's name or other identifying information. Records "blurring" is a reduction of the capability to identify the individual student via collecting data into categories, or aggregating across small groups, or reporting rounded values or a range of values instead of exact figures. True de-identification is the process of removing or obscuring any PII so there is no reasonable basis for believing an individual could be identified from the remaining information.

The Privacy Technical Assistance Center of the U.S. Department of Education has said:

> ". . . simple removal of direct identifiers from the data to be released DOES NOT constitute adequate de-identification. Properly performed de-identification involves removing or obscuring all identifiable information until all data that can lead to individual identification have been expunged or removed."

De-identification of current data must also take into account prior data (either released or properly considered "directory information") in order to confirm that the series of releases, combined, cannot lead to identification of any individual. At the same time, codes that are not student identifiers can be attached to de-identified data so that an individual's performance can be tracked without the tracker being able to identify the individual. Data that has been properly de-identified may be shared without consent of the parent/guardian or student.[9]

IV. RECOGNIZED DISCLOSURE EXCEPTIONS UNDER FERPA

Except in the limited circumstances identified in FERPA and state rules, PII may not be disclosed without consent.[10] Even when a district's disclosure to a cloud vendor is authorized, the

[9] 34 CFR, Section 99.31(b).

[10] A district may disclose PII from the education records of a student without obtaining prior written consent of the parents or the eligible student, including:
- To other school officials, including teachers, contractors, vendors, consultants, and others who have legitimate educational interests, or other parties under the direction and control of the school to whom the school has outsourced institutional services or functions otherwise performed by employees with legitimate educational interests. (34 CFR, Section 99.31(a)(1))
- If annual notice has been given, to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled, if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of Section 99.34. (34 CFR, Section 99.31(a)(2))
- To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or state and local educational authorities in connection with an audit or evaluation of federal/ state-supported education programs. (34 CFR, Sections 99.31(a)(3) and 99.35)
- In connection with specified activities for financial aid. (34 CFR, Section 99.31(a)(4))
- To state and local officials or authorities to whom information is specifically authorized under a state statute that concerns the juvenile justice system. (34 CFR, Section 99.31(a)(5))
- To organizations conducting studies for, or on behalf of, the school in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (34 CFR, Section 99.31(a)(6))
- To accrediting organizations. (34 CFR, Section 99.31(a)(7))
- Under a judicial order or lawfully issued subpoena. (34 CFR, Section 99.31(a)(9))

vendor's uses of the data are also controlled and no redisclosure is permitted except within the acceptable guidelines discussed below. Because it seems unlikely that a school district would de-identify data in order to put it into the cloud, and would most likely be using the cloud in connection with data that included PII, we will be discussing the FERPA exceptions permitting such PII-loaded data and the permitted uses by the cloud vendor. The two FERPA exceptions that are the primary source of cloud computing authorization are "directory information" and "school official."

Under the "directory information" exception, contained in 34 CFR 99.31(a)(11), certain data declared by the district to be part of directory information may be shared with those types of agencies listed in the district's Annual Notice to Parents. Portions of the definition of "directory information" seem to apply directly to the concept of data access, whether in the cloud or on district property. "Directory information" is defined in FERPA regulations as:

> "'Directory information' means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed.
>
> (a) Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended.
>
> (b) Directory information does not include a student's –
>
> (1) Social security number; or
>
> (2) Student identification (ID) number, except as provided in paragraph (c) of this definition.
>
> (c) In accordance with paragraphs (a) and (b) of this definition, directory information includes –
>
> (1) A student ID number, user ID, or other unique personal identifier used by a student for purposes of accessing or communicating in electronic systems, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a personal identification number (PIN), password or other factor known or possessed only by the authorized user; and
>
> (2) A student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that

---

- In connection with a health or safety emergency. (34 CFR, Section 99.31(a)(10)
- Directory Information. (34 CFR, Section 99.31(a)(11))

> authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user."[11]

There are several limitations on use of the "directory information" exception, including the limitation on what PII is considered "directory information" (only information that can be disclosed without harm may be deemed directory information). For all practical purposes, this would preclude use of the exception as authority to place the entire student information system, or even the student attendance system, into the cloud as it appears other information in those systems would be harmful to students if released.

An additional limitation to the use of "directory information" is the ability of individual families to opt out of disclosure of "directory information." Some cloud usage (as with a provider's online product that requires student login access) may be covered by the "directory information" exception since the typical login information is considered "directory information. " However, the typical login requirement (that there also be a PIN or other identifier known only by the person logging in) could still create a disclosure issue as we believe the cloud vendor needs the student's name or number in connection with the PIN or other identifier in order to set up the login, and the PIN or other identifier is outside the definition of "directory information" permitted under this exception.

The more commonly used and beneficial FERPA exception for use of cloud vendors is the "school official" exception. This is the same exception that allows district staff, including teachers and others who have an educational interest, to access confidential student records.[12] The definition of "school official" expressly includes outside contractors, with restrictions. For example, only outside contractors who perform institutional functions that would otherwise be performed by employees and who are under the control of the district and subject to the same use and redisclosure restrictions, qualify as "school officials."[13] As stated in the regulations:

> "An educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests. An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective and that it remains in compliance with the legitimate educational interest requirement in paragraph (a)(1)(i)(A) of this section."[14]

---

[11]20 USC, Section 1232g(a)(5)(A)).

[12]34 CFR, Section 99.31(a)(1)(i)(A).

[13]34 CFR, Section 99.31(a)(1)(i)(B).

[14]34 CFR, Section 99.31(a)(ii)).

The district must also have described to parents/guardians, in the district's annual notice, the criteria on which the "school official" determination is being made.[15] The Schools Legal Service template for Annual Notice to Parents complies with this requirement, as well as with the requirement to discuss "directory information" categories.

V. REUSE AND REDISCLOSURE RESTRICTIONS

It is necessary to discuss a cloud vendor's reuse and redisclosure restrictions because of the practices of some cloud vendors of "data mining" their own cloud for information of commercial value to them. Some data mined information targets individuals with advertising or other products, and some vendors sell data they collect to third parties for their use. Even if they say they don't, they might be mining district data.[16]

Some uses and some redisclosures are permitted but carefully restricted. Where a district is authorized to disclose data to a vendor qualifying as a "school official," that vendor may use the PII data only for the purpose for which access was given.[17] If access was given, in part, for the vendor to do something with the data and then disclose it on behalf of the district to a third party, that is permitted as well. For example, a district could be obligated to report certain student discipline data to the state and the district's cloud vendor could store the data and also extract from it information for any official reports the district is required to file. That re-disclosure is permitted.

More commonly, cloud vendors may be providing instructional services through their cloud and may be tracking student performance and reporting back to the district. If this is the purpose for which the data is being disclosed in the first place, it would be a fairly clear example of use of the "school official" exception. If the vendor is also under contract to make suggestions for student improvement based on student performance, or to offer additional programs or the like, this too would be permitted.[18] "Directory information" and de-identified information are not

---

[15]"If the educational agency or institution has a policy of disclosing education records under § 99.31 (a) (1), a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest." (34 CFR, Section 99.7(a)(3)(iii))

[16]"Google Admits Data Mining Student Emails in its Free Education Apps" by Jeff Gould, SafeGov.org,, Friday, January 31, 2014: "When it introduced a new privacy policy designed to improve its ability to target users with ads based on data mining of their online activities, Google said the policy didn't apply to students using Google Apps for Education. But recent court filings by Google's lawyers in a California class action lawsuit against Gmail data mining tell a different story: Google now admits that it does data mine student emails for ad-targeting purposes outside of school, even when ad serving in school is turned off, and its controversial consumer privacy policy does apply to Google Apps for Education."

[17]The party that receives PII may use the information only for the purposes for which the disclosure was made. (34 CFR, Section 99.33(a)(2))

[18]34 CFR, Section 99.31(a)(6)(i).

subject to use or redisclosure restrictions; however, this is not where many cloud vendors draw the line on data use.

Many vendors mine the district's data for their own purposes. To the extent they are not expressly authorized to do this by contract, a FERPA violation may be present. This is supposed to be covered under a contract between the district and the vendor, but in many cases the only contract present is the TOS to which the district, or district employee, agreed on accessing and using the vendor's product, and is why it is so important to have rules in place regarding staff's access and use of the myriad online products offered daily. The employee's agreement to the TOS (typically done by mouse click without reading) could expose the district to FERPA violations where the vendor mines data, including PII, from classroom use of the vendor's product. This could arise in the form of a parent's complaint about their student constantly being bombarded with targeted advertising from an online vendor or contacts/advertising from a third party to whom the data was sold by the online vendor. Even if the student and parents/guardians appreciate the contact, there are potential FERPA violations involved.

VI. BEST PRACTICES FOR MEETING FERPA REQUIREMENTS IN THE CLOUD

This cloud discussion is divided into two primary categories: 1) pure data storage, and 2) interactive instructional programs. There may be combinations and other cloud uses, but most issues can be identified within these contexts.

The concept of storage includes the exchange of district-owned servers and storage devices for those of an outside and offsite vendor. The district may place large portions of its data into this form of cloud or be more selective. For example, personnel records, business records, and archives could be moved to the cloud and most of the FERPA issues arising from student records would not be present, although privacy and other concerns would still apply. If student data is also moved to the cloud, FERPA must be addressed. When the data is not simply being stored but is also being constantly modified by multiple users, including teachers, parents, and administrators, the rules are more complex.

Assume the district's use of "cloud computing" is limited to offsite storage of various files, including student records which district employees access remotely and update as needed. School networking professionals nationwide have identified several issues that accompany offsite storage of confidential files, including sharing offsite servers with others. Server sharing can lead to a data breach from faulty maintenance, server updating, patches, or configuration issues resulting in the cloud vendor causing or allowing others to have access to district data.

Are district employees' files, including names, maintained in the cloud? What about social security or driver's license numbers or their office-issued credit card or medical or health information? A security breach of an individual's name in combination with any one or more of those items constitutes a security breach for purposes of the Information Security Act and the district must notify the employees whose data may have been compromised each time there is a breach. The same notice requirement applies for any security breach involving student PII.

A security breach can arise from faulty configuration of the cloud servers, through which unauthorized individuals (who share the same cloud server) could obtain access to district files, or where the data is uploaded by school staff to a "shared" rather than a "secure" space on the cloud server. Either way, the district has experienced a data security breach, notice of the breach is required, and the privacy and FERPA issues must be addressed. Imagine the board meeting the month after you've given notice to every student that their confidential data has been breached in the cloud.

Now, imagine the district's cloud vendor searches for and extracts data or metadata from its digital records for the purpose of targeted advertising and/or selling to others to perform that task. While the cloud vendor may have access to the records to perform functions required to manage the stored data, this may not be the vendor's only intent. The vendor's access and/or use of PII outside the scope of their responsibilities could be a FERPA violation.

Many districts have student information systems that permit parental and/or student logins for multiple reasons. User names and passwords, both of which are considered PII, are being disclosed to or handled by the cloud vendor, which means the district must find one of the permitted uses in FERPA to authorize the release of PII. The "school official" exception is the one typically used. The district is authorized to disclose PII to a vendor when the vendor provides a legitimate institutional service or function, is under direct control of the district, and is subject to the use and disclosure limitations of FERPA.[19]

When a vendor has lawful access to PII, they can only access the PII for the identified institutional purpose. This may become problematic when the vendor wants to use the data for its own unrelated purpose, which may be to sell advertising or to sell the data. This is not permitted where PII is involved.

De-identified data has different rules but when student records are stored in the cloud they include PII; mining of that data, even if extracting only de-identified data, violates FERPA unless the mining of the PII-included data meets one of the recognized exceptions. The exception typically employed is performing a study to improve instruction.[20] This exception requires a written agreement spelling out the need/request for and the nature of the study. No other use of the mined data is permitted unless it also meets another recognized exception. There is some question whether this exception applies to the "pure storage" cloud function and the contract (not the TOS) between the district and vendor sets up the scope of services.

Again, student information that has been de-identified or shared under the "directory information" exception is not protected by FERPA and is not subject to use and redisclosure limitations. However, "directory information" is only to be shared in accordance with the contents

[19]34 CFR, Section 99.31(a)(1)(i)(B).

[20]34 CFR, Section 99.31(a)(6).

of the district's annual notice on such information. Once shared, the organization receiving the "directory information" is not under any restriction on redisclosure of the information unless the district imposes a limitation on reuse in the contract. Consider whether the parents receiving the district's annual notice would appreciate your restricting the unlimited redisclosure of the "directory information."

In the case of interactive instructional/educational programs in the cloud, these are typically allowed under the "school official" exception if described in the district's annual notice and if the other requirements are met. These programs may include email and may be web-based educational software or similar programs. There is an assumption of interaction, whether it is sending and receiving email, learning via an online resource, or viewing/grading results, tests, quizzes, or other projects done online. It is assumed the data accessible to the online vendor includes PII, such as student names, email addresses, parent names, and identification numbers that may be indirect identifiers and which may include a PIN or other login data required to access the program. Use of that vendor's program could also include reports back to the district on certain data collected for use in assessing a student's use of the program. Examples could be reporting the duration of time spent logged onto a particular page or subject, the amount of time a cursor hovered over an answer, and a myriad of other metadata that could provide some educational value to the district. All these subjects appear to involve data linked to an identified student but fall within the context of legitimate educational purpose and are not an issue.

In such instances, districts may also contract with the vendor for suggestions relating to improved use of the cloud program, ways to increase student use and/or achievement, and information on other programs that may be of value to the district's educational programs. This use is absolutely permitted under FERPA and if the district's cloud vendor has "partners" who participate in that process, redisclosure to them is also permitted, though limited.[21]

However, some cloud vendors engage in the mining of PII-included data for their own purposes, such as targeted advertising or other sales, marketing, or related purposes, and sometimes redisclose extracted data to third party partners or buyers. This is not legal, even if included in the vendor's TOS and especially not if such rights are expressly excluded in an appropriate contract. The U.S. Department of Education's Privacy Technical Assistance Center's February 2014 publication "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" speaks of this vendor practice as follows:

> "On occasion, providers may seek to use the student information they receive or collect through online educational services for other purposes than that for which they received the information, like marketing new products or services to the student, targeting individual students with directed advertisements, or selling the information to a third party. If the school or district has shared information under FERPA's school

[21] 34 CFR, Section 99.31(a)(1), (a)(6), and (b)(1).

official exception, however, the provider cannot use the FERPA-protected information for any other purpose than the purpose for which it was disclosed.

Any PII from students' education records that the provider receives under FERPA's school official exception may only be used for the specific purpose for which it was disclosed (i.e., to perform the outsourced institutional service or function, and the school or district must have direct control over the use and maintenance of the PII by the provider receiving the PII). Further, under FERPA's school official exception, the provider may not share (or sell) FERPA-protected information, or re-use it for any other purposes, except as directed by the school or district and as permitted by FERPA.

It is important to remember, however, that student information that has been properly de-identified or that is shared under the 'directory information' exception, is not protected by FERPA, and thus is not subject to FERPA's use and re-disclosure limitations."

As noted, this issue is not present if the data has been properly de-identified or was "directory information," but the district could still restrict or preclude such activities via the vendor contract if the vendor agrees.

VII. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

The restrictions imposed by FERPA on the use and redisclosure of PII are not the only rules applicable to the cloud environment. The Children's Online Privacy Protection Act (COPPA) also deals with the privacy of personal information pertaining to children under age 13. The potential for issues is clear when there is an understanding of what constitutes "personal information" for purposes of COPPA. "Personal information" under COPPA includes:

"First and last name;
A home or other physical address including street name and name of a city or town;
Online contact information;
A screen or user name that functions as online contact information;
A telephone number;
A social security number;
A persistent identifier that can be used to recognize a user over time and across different websites or online services;
A photograph, video, or audio file, where such file contains a child's image or voice;
Geolocation information sufficient to identify street name and name of a city or town; or
Information concerning the child or the parents of that child that the operator collects online f

As can be seen, the types of information considered to be "personal information" under COPPA are routinely found in many online activities. COPPA expressly applies to operators of commercial websites and online services (including mobile apps) directed at children under 13 that collect, use, or disclose personal information from those children. The rules also apply to websites

or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.[22]

COPPA requires parental consent for the collection, use, or disclosure of personal information. When a cloud vendor operates under the "school official" exception to FERPA, parental consent is not needed, but that exception only covers permitted uses of the data. Under COPPA, a vendor's collection, use, and re-disclosure is permissible if allowed by their contract, under which they may assume parental consent is present or not needed. However, when a vendor exceeds the permitted scope of the district's consent, parental consent is required.

As one author has stated:

> ". . . 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.' 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.' 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."[23]

At the very least, this should require clarity in the required contract over what information constitutes personal information and what uses and redisclosures are and are not permitted. It is not clear how targeted advertising could be "targeted" unless the vendor or third party knows the identity of the target and the "need" for the products being marketed. This knowledge appears to include PII. Any intended commercial use of school data should be discussed beforehand.

VIII. WRITTEN CONTRACT REQUIREMENTS

For the "school official" exception to be valid, the cloud vendor must be "under the direct control" of the district.[24] The only way an independent contractor can be said to be "under the direct control" of the district is for there to be a contract establishing that control. Additionally,

---

[22]COPPA FAQ - Question A2.

[23]"Cloud Computing, Regulatory Compliance and Student Privacy: A Guide for School Administrators and Legal Counsel" by Steve Mutkoski, Microsoft Corporation, presented at the Council of School Attorneys National School Law Meeting, October 10-12, 2013.

[24]34 CFR, Section 99.31(a)(1)(i)(B)(2).

the exception for doing studies expressly requires a written agreement,[25] as does the exception for audits and evaluations of state or federal programs.[26]

When a district enrolls in an online instructional program, there likely will be some form of licensing agreement which could also be used to meet the requirements of FERPA. The bigger problem is when individual district employees sign up for software (apps) without district knowledge or consent and use them in the classroom, perhaps having students use the program as well. As with most apps, many online programs only require the user to click the "accept" button as to the vendors' TOS and begin use. Agreeing to the TOS may not meet all the requirements of FERPA and may grant rights to the vendor that FERPA does not allow.[27]

The contract should include the following points:

A. The factual basis for the disclosure by the district to the vendor - why the district desires to use the vendor's services - and designation of the vendor as an authorized representative.

B. The scope of services - exactly what the vendor is under contract to perform and the specific purposes for which PII may be used.

C. To the extent identified, activities for which the vendor is not authorized.

D. What data may be used, and what data may not be used, as applicable.

E. Specification of any third parties to whom the vendor may redisclose data in the course of performing the scope of work, the basis and limitations for such redisclosure, and assurances the data will not be redisclosed by the third parties or disclosed to unidentified third parties.

F. The purpose of any permitted data collection, use, and/or redisclosure for reasons outside the contracted scope of services, the basis and limitations for such collection, use, and/or redisclosure, and assurances the data will not be redisclosed by the identified third parties or be redisclosed by the vendor to unidentified third parties.

G. The time limits and dates, if any apply, by which the data is to be returned or deleted by the vendor and approved methods of destruction.

[25]34 CFR, Section 99.31(a)(6)(iii)(C).

[26]34 CFR, Section 99.35(a)(3).

[27]For this reason, we strongly suggest that districts limit staff's ability to use any form of app or software that is not district-approved with an approved vendor contract.

H. Provisions for reporting data breaches and responsibility for same in the party causing/allowing the breach.

I. Provisions for penalties to be applied to any violation of the contract by the vendor or third party to whom the vendor rediscloses data.

J. Standard provisions on vendor's compliance with all applicable laws, the district's right to audit vendor's records, pricing, conflict resolution, indemnity, insurance (including coverage for costs/damages for data breach/loss), and application of U.S. and/or California laws with jurisdiction and venue for disputes in the county where the district is located.

IX. CONCLUSION

Computing in the cloud, whether simple data storage or more complex instructional or educational functions, is a rapidly expanding frontier and the players are just getting used to the challenges they face with existing technology. While there are dangers and numerous requirements to using cloud services, there are many more benefits; this is the present in which schools must operate in order to remain competitive, in order to expand choices and opportunities for learning, and in order to keep up with the increasing capabilities and capacities of both staff and students.

This, however, is not the future. As reported by the Wall Street Journal, the future is not the cloud but what they call the "fog." According to them, the future will be found not in large servers but in the multitude of small and mobile devices that will be tasked with doing more and more of the computing. They describe the future this way:

> ". . . in the world of mass connectivity—in which people need to get information on an array of mobile devices—bandwidth is pretty slow. Any business that sends data to mobile devices, be it airline reservation systems for consumers or business data for a mobile sales force, grapples with the limitations of wireless networks . . . . That's one reason that mobile apps have become a predominant way to do things on the Internet, at least on smart-phones. Some of the data and processing power is handled within your device . . . . Whereas the cloud is 'up there' in the sky somewhere, distant and remote and deliberately abstracted, the 'fog' is close to the ground, right where things are getting done. It consists not of powerful servers, but weaker and more dispersed computers of the sort that are making their way into appliances, factories, cars, street lights and every other piece of our material culture."

Even though it's still summer, it's time to begin thinking about the "fog."[28]

[28] "Forget 'the Cloud;' 'the Fog' is Tech's Future" by Christopher Mims, Wall Street Journal Online, May 18, 2014.