Data Privacy Law Update: Ten Things to Advise Your School Board Clients – Before It’s Too Late

David Rubin, David B. Rubin PC, Metuchen, NJ; Phil Hartley, Harben, Hartley & Hawkins, Gainesville, GA; Sonja Trainor, Director, NSBA Council of School Attorneys

Presented at the 2016 School Law Practice Seminar, October 20-22, Portland, OR

The NSBA Council of School Attorneys is grateful for the written contributions of its members. Because Seminar papers are published without substantive review, they are not official statements of NSBA/COSA, and NSBA/COSA is not responsible for their accuracy. Opinions or positions expressed in Seminar papers are those of the author and should not be considered legal advice.

© 2016 National School Boards Association. All rights reserved.
State legislatures are rapidly adopting laws governing student data privacy and security. According to information reported by the National Association of State Boards of Education, in 2014, 110 bills related to student data privacy were introduced in 36 states. In 2015, it was 188 bills in 48 states. In 2016 thus far, we have 11 bills in 34 states. Thirty-five states have passed 73 laws since 2013.

The U.S. Department of Education’s Privacy Technical Assistance Center has issued numerous guidance documents and offers trainings.1 The White House has issued several reports,2 and President Obama even referenced the importance of student data privacy in a State of the Union address. Although Congress isn’t passing much right now, it did nod toward student data privacy in the remarkable bi-partisan re-do of No Child Left Behind, December 2015’s Every Student Succeeds Act3 by requiring grant recipients to understand that they are subject to the requirements of the Family Educational Rights and Privacy Act (FERPA),4 prohibiting a national database of student personally identifiable information, and allowing Title II professional development grants to be used for activities including data literacy and data privacy training.

If your state has not yet adopted student data privacy legislation, it likely will soon. And it is reasonable to assume that Congress will eventually update FERPA, separate or apart from new provisions addressing educational data service providers, online operators of websites aimed at children, and data security. In the meantime, educational, data privacy, and tech industry groups have produced reams of valuable resources, shared principles, and a Pledge that subjects vendors to FTC jurisdiction. Consortia of school districts have formed to put out standard contract addenda particular to their jurisdiction.

For now, there is plenty of “good practice” guidance and trends in the law to formulate some key points you should be making to your school district clients, even if your state has not passed its own student data privacy law. We offer these, as well as the resources listed in the Addendum, as a summary of the current thinking. We urge you to remain current with this rapidly-evolving area of law by checking in frequently with the Council of School Attorneys’ web pages and email groups, and with the organizations listed in the Addendum.

1. **Think in terms of “data,” not “records.”**

One need not look far for examples of educational terminology that has become obsolete. When Congress first adopted groundbreaking legislation, in the 70’s, to assure “handicapped” children had access to an

---

3 P.L. 114-95 (December 2015).
education, no one envisioned the baggage that would weigh down that term years later. So too with “records,” the term typically used by school board counsel when analyzing clients’ obligations to protect student privacy.

“Education records” was the phrase chosen by Congress in FERPA\(^5\) to describe what information must be safeguarded, but that statute was adopted in 1974, almost 20 years before the advent of the Internet. “Education records” were defined as “records, files, documents, and other materials[,]\(^6\) reflecting the hard-copy recordkeeping practices of the day. The FERPA regulations\(^7\) broadened that definition somewhat to include “information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.” Yet even those terms are antiquated by today’s standards, considering how much information is now exchanged or maintained in e-mail, cloud storage, text-messaging, or teachers’ phone apps.

Aligning school district privacy practices with the realities of the digital age will require a shift in our clients’ mindset. The sorts of “records” envisioned by FERPA are now relics of a bygone era. School districts must broaden their field of vision to encompass the full range of student data swirling around them, not only on campus but off-site in the hands of educational service providers. This wider perspective is urgently needed, given our clients’ increasing reliance on student data to make better-informed policy decisions at the board, and to help teachers more precisely target individual students’ needs. The challenge is to reap the full benefits of this information, while assuring the security and privacy of all student information in our clients’ control.

2. **Know where your student data is going and under what authority.**

When student records in filing cabinets are replaced by data, whether personally identifiable or not, stored somewhere in the Cloud, all kinds of legal concerns arise, especially when lawyers begin to consider where all that data is going. School districts and their legal counsel need to be able to answer those questions because parents expect answers, and legal challenges of the future will demand answers. One of the provisions frequently contained in state legislation being passed in the last few years is a requirement for a student data audit. As an example, Georgia’s Student Data Privacy, Accessibility and Transparency Act\(^8\) requires the State Department of Education to create and make available a “data inventory” identifying student data required to be reported by the State, required to be reported by the Federal Government, collected as a part of the State-wide Longitudinal Data System (and why it is being collected) and collected by the State “with no current identified purpose.” While the Georgia law does not currently require that each local district conduct a similar inventory, it is a strong recommendation of the U.S. Department of Education’s Privacy Technical Assistance Center.\(^9\) Without a baseline audit, school districts lack a vital foundation on which to address student privacy, security and transparency concerns. Creating and maintaining such an audit in most school districts virtually requires a dedicated assignment

---

\(^5\) 20 U.S.C. § 1232g.
\(^7\) 34 C.F.R. § 99.3.
\(^8\) O.C.G.A. §§ 20-2-660 through 668.
of someone as a Chief Privacy Officer, another of the requirements of many state laws, including Georgia’s.

Of course, one of the many advantages of technology is the ease with which information can be shared. In many states, recent federal and state accountability legislation, regulations and grants have led to the development of a state-wide longitudinal data system in which local districts are required to participate. To facilitate the use of such a system, it is integrated or synchronized with other district programs and school employees quickly lose any awareness of what data is required to be created and maintained by some legal mandate and what data is being created and maintained because of school or even teacher programs. Student data of different kinds is also frequently provided in personally identifiable or de-identified form to other state or local agencies usually directly from the local district, but sometimes by access to the state longitudinal system. Sometimes this involves other educational agencies with non-student purposes (teacher certification, teacher evaluation, accountability at the district and school level, funding, etc.), but school officials rarely make the effort to determine what student data, in what form (PII or otherwise), must be provided and by what authority. Such analysis becomes even more complex when the data is being provided to non-educational entities that serve the same student population (think Family and Children Services, law enforcement entities, Department of Driver Services, local health clinics, mentoring agencies and others). The ability to download and email or text creates greater ease of communication and greater opportunity for data to get distributed in ways that make security more difficult. Ideally, the inventory described above would also include identifying what data goes where so that everyone understands the nature of the data that has to be provided, what should not be provided, and how any responsibility to protect privacy transfers to the receiving agency.

As noted, student data today is more than just permanent record transcripts, class rosters, and discipline slips; instead, most of the instruction and services provided to a student is done electronically by virtue of programs created by and contracts entered into with private vendors. The importance of legally-reviewed contracts that not only implement the school official exception of FERPA, but also clearly address who has access to the data, who controls this data, how it can be accessed by others, including parents to the extent it is personally identifiable and qualifies as an educational record, cannot be overemphasized. Many parents are concerned that their child’s data is being used by the vendor or a customer of the vendor for other purposes. Since the Student Data Privacy Pledge was originated in October 2014, most providers have agreed, some more reluctantly than others, to voluntarily abide by the commitments in the Pledge. These basically include that student information will not be sold, students will not be targeted for advertising, data will be secure and accessible to parents, and data will be used for educational purposes only.

School districts and parents are now learning that in this interconnected world, a student’s or teacher’s access to one product that may be covered by the Pledge may create or allow access to other products not covered. In a complaint filed with the Federal Trade Commission, the Electronic Frontier Foundation accused Google of unfair trade practices in providing schools with Google Apps for Education apparently in conformance with the Pledge and Chromebooks for individual student use. The allegations in the complaint are that by providing a common user name for students and default access to Google Chrome, a broader consumer program not covered by the Pledge, Google continues to gather and use data from students in a way not contemplated by the purest interpretation of the Pledge. Of particular interest is

---

10 34 C.F.R. § 99.31(a)(1)(1).
one allegation that Google allows an administrative setting by a school district that allows an interface with other third-party websites. While the Google case may be high profile now, privacy groups have similar suspicions regarding products from Microsoft, Apple, FaceBook and others. More importantly, school districts need to understand the technological as well as the legal fine print when purchasing software or other services. Interconnectivity and the ability to communicate and work across platforms and programs is the essence of today’s internet universe. What does it say about education if it is bucking the trend? As noted in questions below, part of the answer is transparency so that parents have the information and cannot claim that they understood that privacy was guaranteed for their child’s school work only to learn that it is as available as their FaceBook page at home.

3. **Make necessary adjustments now to increase security and accessibility of data.**

School data security is a highly technical field, but here are just a few of the tips that the experts recommend to increase security of student information without unnecessarily compromising accessibility.

Alert the school community to the district’s expectations by adopting a clearly-worded Acceptable Use Policy governing all online activity, both internally and on the Internet. Consider incorporating school security policies into staff job descriptions, and assign specific individuals to monitor compliance. Computers housing sensitive data should be made physically inaccessible to unauthorized users, unnecessary services should be shut down, and staff should be trained to report lost or stolen equipment immediately.

All computing devices in the district should be inventoried, with network mapping implemented to provide an understanding of how the components of the system interconnect. Proper authorization protocols are critical, with two-factor authentication preferable where possible, especially for web-accessible log-in. At a minimum, “strong” passwords should be required. Firewalls alone may be inadequate to protect the district’s system, so multi-layered “Defense in Depth” architecture is recommended. Ideally, full-disk encryption should be required for all computing devices, servers and portable storage media.

More in-depth guidance is available in the school-friendly publications of the U.S. Department of Education’s Privacy Technical Assistance Center and the Future of Privacy Forum, a D.C. think tank, available online.11

4. **Be transparent about where your student data is going, how it’s maintained and by whom, how it’s disclosed, and under what conditions it’s destroyed.**

In addition to privacy and security, transparency is viewed as a critical piece of a school district’s responsibility in handling student data. Of course, since 1974, FERPA has imposed on school districts the requirement to keep student records confidential, yet available upon request to parents. Many states mandate that information be provided to parents regarding how to access their child’s data, and many of those states require access to instructional materials and de-identified or aggregated data in addition to

---

their own child’s PII. Privacy advocates strongly contend that districts should model transparency by providing links on websites and easy access to all policies, regulations, and especially complaint procedures related to student data. From the USED’s PTAC, “the Department recommends that schools and districts clearly explain on their Websites how and with whom they share student data, and that they post any school and district policies on outsourcing of school functions, including online educational services. Schools and districts may also want to post copies of the privacy and security provisions of important third party contracts.”12 At a minimum, someone, and hopefully multiple someones, should be able to answer parent questions.

As with any contract between a private vendor and the school district, the open records or freedom of information statutes of each state provide the parameters of what has to be provided and what limitations, such as trade secrets or proprietary information, might exist. As noted above, when disclosure turns to the specific data relevant to an individual student, issues can get more complicated. With the proliferation of state statutes and the anticipated rewriting of FERPA, it is conceivable that school districts will be dealing with multiple definitions applicable to different situations. Much of the student data created today is also used for other purposes ranging from teacher evaluations to school accountability ratings to research by the vendor to improve the product. Even where this data is allegedly de-identified and then aggregated, parents have concerns about when it becomes a part of a student’s record, or an open record under state law or otherwise protected from disclosure, for example as part of an individual teacher’s evaluation.

Thinking of data rather than records also creates new headaches in the area of records retention and destruction. If data is part of a student’s record, then there may exist specific records retention requirements under state law that it be maintained for some extended period of time. IDEA has long had a requirement that notice be given to parents when PII is no longer needed to provide services to a student and that such records be destroyed upon parental request.13 Part of the requirement that a school district exercise control over an outside vendor being treated as a “school official” under FERPA is that the vendor agrees to destroy PII upon request of the district.14 Parents, who feel entitled to question every grade, student class ranking and other aspect of their child’s education, may insist on reviewing the data, or even the metadata, applicable to the decision and not just the summative report generated to explain how their child performed on a specific assignment. Thus, school board attorneys have to be aware of, or at least be able to find, the relevant legal requirement and the vendor contract that may indicate where the requested data is maintained and whether the vendor or district controls access to de-identified or aggregated data and metadata.

Of course, in addition to the legal issues, technology issues also complicate questions regarding retention and destruction of such data. Lawyers have learned through e-discovery controversies that deleting information in a computer network is often not as easy as it seems. Even where the school district intends to have eliminated specific data or records, contracts have to be reviewed to determine whether the vendor maintains copies, or whether the ubiquitous Cloud could make such data accessible under some

13 34 C.F.R. § 300.624(a) and (b).
14 34 C.F.R. § 99.31(a)(1)(1).
circumstances and whose obligation it would be to retrieve it. This may involve posting vendor contracts on the school district website, as well as clear descriptions of policies and procedures, and an FAQ on the school district website. Staff should be able to respond to parent questions.

5. **Know your state requirements for parent choice, and opt-out/in of data disclosure and have clear policies.**

Related to transparency, but with its own set of issues, is the question of parent choice. FERPA currently provides the classical template: certain information (directory information under FERPA\(^{15}\)) parents control and can choose to keep confidential outside the school environment. Within the educational function, parents have access to whatever records are created by the district and have a process to correct errors that may exist,\(^{16}\) but cannot control the specifics of records that are created for instructional purposes and, with a few exceptions that have developed in many states such as sex education, cannot control the instructional materials used. The Protection of Pupil Rights Amendment\(^{17}\) regulates the gathering of certain data or information; political affiliation, family beliefs, religious views, and others without parental permission. Many state statutes have also adopted the latter approach with regard to certain topics in an attempt to keep “government” out of the personal lives of students and parents.

With parent choice rights expanding in so many areas (school assignments and mandated testing), many parents believe that they have some Constitutional right to control every aspect of their child’s education in a public school. School district attorneys are used to getting demanding letters opting out of testing, certain curriculum, counseling, discipline, and other areas. With the focus on student privacy and transparency, policy development and communication to parents in this area is essential. Parents need to understand their rights and a process needs to be carefully defined for correcting records that are wrong and for processing complaints by parents who contend that policies or records laws have been violated. At the same time, with the large majority of instruction taking place online and at least aggregated data being used for non-student purposes from teacher evaluation to establishing compliance with federal statutes, local policies should be very careful about granting or even implying that parents have a right to opt out of instructional methodologies, courses, assessments or reporting requirements. As many states and districts are experiencing with the testing opt-out movement, if parents can choose not to have their individual children participate, the value of technology as a tool for student improvement and more efficient instruction quickly disappears.

6. **Adopt clear and well-communicated policies and procedures regarding purchasing and using hardware, software, and online educational tools (apps).**

Because educational institutions are required under FERPA to retain direct control over third parties that access, use, and maintain student personally identifiable information contained in student records,\(^{18}\) a school district should communicate clearly to staff its expectations and policies for adoption and use of any electronic platform, including online apps.

---

\(^{15}\) 34 C.F.R. § 99.3.
\(^{16}\) 34 C.F.R. §§ 99.21, 99.22.
\(^{17}\) 20 U.S.C. § 1232h.
\(^{18}\) 34 C.F.R. § 99.31(a).
The National Forum on Education Statistics Guide to Education Data Privacy\textsuperscript{19} describes two approaches for pre-use approval of classroom online services and apps: decentralized and centralized review. The former, often used in districts without central office staff and resources to review every app prior to use, affords teachers a great deal of freedom to adopt and use apps in the classroom that they believe are helpful tools for their students. The district employing this approach offers guidance to teachers on choosing apps that address instructional, privacy, and security concerns. Some also require teachers to get parent consent before using an online app, thus alleviating the FERPA problem. The Guide lists detailed guidelines for reviewing online instructional apps for privacy, including:

- Student academic information should be password-protected or controlled by teacher invitation—not available for discovery through search engines.
- PII like a student name, email address, or student identifier likely require parent consent (especially when used in conjunction with academic information).
- Review the Terms of Service for specific provisions like age restrictions, security measures, and more.\textsuperscript{20}

In a centralized review framework, the district has a list of pre-approved online apps for use in the classroom, and/or strong contract addenda with vendors. All staff authorized to negotiated contracts must do so consistently, using the same form agreements.\textsuperscript{21}

\textbf{ONLINE INSTRUCTIONAL APP TOS/PRIVACY POLICY CHECKLIST*}

Age restrictions: if the platform is intended for children 13 or over, it should not be used for younger students.

Student data should be securely maintained, used only for educational purposes, and not shared with other organizations.

The provider should not be permitted to make material changes to the TOS or privacy policy without notice/consent of the district.

Student data should not be used to advertise or market to students.

PII should be defined broadly.

Be wary of permitting uses of “de-identified” data.

Be wary of allowing access through a third-party site.

Types of data collected should be specified.

TOS should agree with all applicable law.


\textsuperscript{20} Forum Guide to Education Data Privacy, supra note 19 at 23.

\textsuperscript{21} Id. at 26.
One step school districts can add to their review of networked and online learning tools is to check whether the vendor has signed off on the Student Data Privacy Pledge.\textsuperscript{22}

Note that the FTC recommends a centralized approach, at least with respect to school district consent for student use of websites that are aimed at students under 13. In its FAQ on COPAA, the FTC notes “As a best practice, we recommend that schools or school districts decide whether a particular site’s or service’s information practices are appropriate, rather than delegating that decision to the teacher. Many schools have a process for assessing sites’ and services’ practices so that this task does not fall on individual teachers’ shoulders.”\textsuperscript{23}

Policies and contract terms should be developed and implemented by staff with student/instructional/privacy background, in addition to your legal counsel.

Recently, consortia of school districts have formed to develop and implement with vendors in their jurisdictions to use common student data contracts and addenda. The Massachusetts Student Privacy Alliance (MSPA), a group of Massachusetts school districts, sets standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations. This consortium has produced a “common Student Data Privacy Agreement to be used by all member schools when implementing any online application. By adopting such a contract, all vendors and schools have common expectations when entering into a relationship or implementation without having to renegotiate terms in every new instance.”\textsuperscript{24} Similar initiatives are in the works in other states.

The Student Data Privacy Consortium, a non-profit collaborative of schools, districts, state agencies, vendors and others formed under the Access 4 Learning (A4L) Community, is producing contracts, templates, and other resources for schools developing student data governance structures. The first project will be a “Privacy Contract Framework,” so that districts and vendors can share model contracts. According to a recent press release, work is underway in several large districts, and statewide collaborative groups in CA, VA, MA, WI, RI and ME.\textsuperscript{25}

Many organizations have tools that school districts can use as a first step to examine applications for classroom use. Common Sense Media, for example, conducts privacy evaluations for apps through its Graphite program. \url{https://privacy.graphite.org/}


\textsuperscript{22} \url{https://studentprivacypledge.org/}.
\textsuperscript{24} \url{https://secure2.cpsd.us/mspa/about_mspa.php}.
\textsuperscript{25} \url{http://www.A4L.org}.
7. Limit vendor use of student data according to widely-accepted parameters.

Certain parameters are now common in state law (GA, CA), are reflected in the Student Data Privacy Pledge and the Student Data Privacy Principles, and are likely to be reflected in any federal law to be adopted in the near future. As described in Section 6 above, school districts are starting to organize into consortia within a jurisdiction to develop standard contract addenda with vendors addressing student privacy.

California paved with way for standard privacy terms in vendor contracts with a set of laws passed in 2014, which place requirements and restrictions on local educational agencies and vendors targeting schools and students. Under the new requirements, LEAs’ technology services agreements must contain certain provisions. Fagen Friedman & Fulfrost’s guide lists these requirements as:

- A statement that pupil records continue to be the property of and under the control of the school district;
- A description of the means by which pupils may retain possession and control of their own pupil-generated content, if applicable, including options by which a pupil may transfer pupil-generated content to a personal account;
- A prohibition against the third party using any information in the pupil record for any purpose other than those required or specifically permitted by the contract;
- A description of the procedures by which a parent, legal guardian, or eligible pupil may review personally identifiable information in the pupil’s records and correct erroneous information;
- A description of the actions the third party will take—including the designation and training of responsible individuals—to ensure the security and confidentiality of pupil records;
- A description of the procedures for notifying the affected parent, legal guardian, or eligible pupil in the event of an unauthorized disclosure of the pupil’s records;
- A certification that a pupil’s records shall not be retained or available to the third party upon completion of the terms of the contract and a description of how that certification will be enforced (NOTE: This requirement does not apply to pupil-generated content if the pupil chooses to establish or maintain an account with the third party for the purpose of storing that content, either by retaining possession and control of their own pupil-generated content, or by transferring pupil-generated content to a personal account.);
- A description of how the district and the third party will jointly ensure compliance with the federal Family Educational Rights and Privacy Act; and
- A prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising.

The CA law actively prohibits operators from disclosing or using student information in specific ways. These prohibitions reflect norms becoming widely accepted, and indeed “codified” in the Student Privacy Pledge. Again, as noted in Fagen Friedman & Fulfrost’s Guide, under the CA law, operators cannot

---

• target advertising on their website or any other website using information acquired from students;
• create a profile for a student, except for school purposes;
• sell a student’s information; or
• disclose student information, unless for legal, regulatory, judicial, safety, or operational improvement reasons.

Operators must:

• protect student information through reasonable security procedures and practices;
• delete school- or district-controlled student information when requested by schools or districts; and
• disclose student information: when required by law; for legitimate research purposes; or for school purposes to educational agencies.

GA and LA have adopted some similar provisions requiring operators to implement protections, and/or LEAs to require specific contract terms with educational service providers. LA prohibits LEAs from sharing information including student names, social security numbers, dates of birth, and addresses, except in limited exceptions, without parental consent.27

If you are reviewing a vendor contract from “scratch,” COSA member Tom Tokarz recommends specific steps and terms, and that you be involved from the initial stages of vendor engagement.28


8. Implement ongoing staff training on data privacy concerns, procedures, policies and parent questions.

In most school districts, protection of electronic data has been relegated to technology coordinators or other highly trained personnel, but staff training is now necessary for all educators to raise awareness of their legal obligations under state and federal student privacy laws, and to curtail inadvertent violations of students’ privacy rights.

The impetus for this training is the proliferation of low- or no-cost educational apps, digital learning tools and other online programs marketed directly to classroom instructors, who innocently click their way through complex terms of service, unaware of the ramifications of the legalese they have just “accepted.” Students’ names, birth dates, grades, behavior patterns, special education classifications and other highly sensitive information are uploaded without any realization that this data has been placed in the hands of vendors with motivations of their own. This typically occurs under the radar, with no centralized oversight

of the procurement process or a prior opportunity for district administrators to orient educators to how this information can be exploited by the $8+ billion “ed tech” industry.

Experts agree that the wave of state legislation recently adopted across the country, beefing up protection of student data and curtailing abuses by technology vendors will come to naught without effective training to curtail the use of apps and programs that have not been properly vetted by authorized district personnel.

9. **Install a dedicated Chief Privacy Officer, Data Governance Committee or office within each district.**

A common thread in best practice recommendations on data privacy, and increasingly reflected in state law on the subject, is the idea of a chief privacy officer, or data privacy committee or office, at the state and increasingly at the local level. New York requires its Department of Education to have in place a chief privacy officer, who must be “qualified by training or experience in state and federal education privacy laws and regulations, civil liberties, information technology, and information security.”

National Forum on Education Statistics’ Guide describes the attributes and processes of an agency’s data governance program -- the overall management of an organization’s data, and outlines policies, standard procedures, responsibilities, and controls at every point in the data life cycle: define, collect, store and protect, use, share, retire. It is reasonable to expect that state and federal regulators will increasingly expect school districts, and even individual schools, to have clear, transparent and well-executed data governance programs. As the Guide notes, this may require more and more cross-agency data planning. In March 2016, the U.S. Department of Education released a Data Sharing Toolkit for Communities, which attempts to clarify how FERPA may allow data-sharing, especially when student information is de-identified and aggregated, to provide wrap-around services to students. On the page entitled “FERPA MythBusters”, the Toolkit notes “Sharing group or grade-level aggregate data can help community partners provide services tailored to student needs.”

PTAC offers a video and checklist for school districts on developing a privacy program, as well as customizable training materials on responding to data breaches.

10. **Be ready for changes to FERPA, including an increased enforcement role for the U.S. Department of Education.**

By the time Congress summons the political will to debate and pass an update to the aging FERPA, or an alternative (or possibly parallel) bill imposing nationwide requirements on ed tech vendors, it seems likely

---

29 NY CLS Educ § 2-d.


32 *Id.* at 14.
the majority of states will have already addressed the topics. As described above, state legislatures have been very active in student data privacy issues in the past few years.

If you and your school district clients are taking the actions listed in 1-9 above, you will be in a good position to be in compliance with any changes to federal law that are likely to be made. It is a good idea to remind your clients that federal legislation has been introduced, and if passed, is likely to include:

- Updates to definitions of terms like “education records” (“maintained electronically or physically”);
- Requirements for schools to have data security and privacy policies;
- Prohibitions on student data being used for marketing or advertising, through contract provisions or direct vendor regulation;
- Transparency practices including posting privacy policies and technology contracts online;
- Reduction in the response time for parent requests (from 45 to 30 days);
- Requirement for public notification of breach;
- Increased enforcement authority of the U.S. Department of Education.

Because states are tackling most of the issues above, perhaps the most significant impact a federal FERPA-re-do may have is the increased authority of the U.S. Department of Education to investigate and impose fines upon federal funds recipients. A House Committee heard testimony in 2014 that school districts are not likely to act with any significant energy until FERPA has enforcement teeth, including fines. Indeed, one bill would allow the Department to impose fines of up to $1.5 million, or 10% of a district’s annual budget.

Some proactive measures, taken now, will put your clients in a better position for the eventuality of increased Department involvement in student data privacy.