EDUCAUSE | LEARNING INITIATIVE

Privacy Considerations in Cloud-Based Teaching and Learning Environments

Veronica Diaz, Associate Director, EDUCAUSE Learning Initiative

Joann Golas, Director of Online Learning, College of Communication, DePaul University

Susan Gautsch, Practitioner Faculty and Director of e-Learning, Graziadio School of Business and Management, Pepperdine University

ELI Paper 3: 2010
November 2010

Abstract

In this white paper, we outline the privacy issues relevant to using cloud-based instructional tools or cloud-based teaching and learning environments for faculty members and those supporting instruction. Our discussion of how teaching and learning in an increasingly technological environment has transformed the way we interact and interpret FERPA will help inform various choices that institutions can consider to best address the law, including policy and best-practice examples. We highlight practical suggestions for how faculty members can continue to use innovative instructional strategies and engage students while considering privacy issues. Finally, this paper discusses ways to further explore and address privacy locally and includes a comprehensive resource list for further reading.

© 2010 EDUCAUSE
This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License.
http://creativecommons.org/licenses/by-nc-nd/3.0/

Privacy in Open, Digital Teaching and Learning Environments

The emergence of a new class of web-based applications, and the ways in which those applications are being incorporated into academic settings, have introduced new possibilities for teaching and learning, but they also bring new concerns about privacy.

The Rise of Web 2.0 Tools

Alongside the rapid growth of e-learning, higher education has witnessed the explosion of Web 2.0 tools and other emerging technologies (Sclater 2008). Web 2.0 tools give users the choice to interact and collaborate with each other in a social media dialogue as creators of user-generated content in a virtual community, in contrast to websites that limited users to the passive viewing of content. Examples of Web 2.0 technologies include social networking sites, blogs, wikis, video-sharing sites, hosted services, web applications, mashups, and tags. These tools, which are typically free or low-cost, represent a transition from institutionally provided to freely available technology.

Web 2.0 or cloud-based technologies in many ways further support a trend that began with the emergence of the Internet: a shift away from large organizational control of the instructional function toward the individual user, both faculty member and learner. These emerging technologies, not necessarily created for higher education consumption, support and require individual creativity and autonomy and foster the growing trend toward user-generated content and knowledge in a way that many institutionally developed products do not. They also have the potential to promote sharing, openness, transparency, and collective knowledge construction. Part of their proliferation can be attributed to the low-cost instructional innovation they enable, along with their ease of use, in a higher education climate of shrinking budgets and increased competition for information technology budget monies. Faculty members and learners no longer need to wait for a learning management system (LMS) to develop and implement a tool, for an institution to purchase a license to use images, or for a streaming media server because many of these needs can now be met externally through a variety of cloud-based tools.

An often overlooked consideration regarding the use of cloud-based tools involves privacy. The Family Educational Rights and Privacy Act of 1974 (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is the federal law that protects the privacy of student education records. Institutional interpretations of what constitutes a "student's education record" vary, but generally, many consider any work related to a course or program of study to fall into this category. Most college and university attorneys, working from the federal regulations, consider the education record to be a broad category that includes or involves study, not just the transcript. Certainly a student's work product is included, but, for instance, an e-mail from a professor about performance is also included. Although FERPA does not prohibit faculty members from using Web 2.0 or other cloud-based tools, some guidelines do apply.

This white paper seeks to outline the privacy issues relevant to using cloud-based instructional tools or cloud-based teaching and learning environments for faculty members and those supporting instruction. Our discussion of how teaching and learning in an increasingly technological environment has transformed the way we interact and interpret FERPA will help inform various choices that institutions can consider to best address the law, including policy and best-practice examples. We highlight practical suggestions for how faculty members can continue to use innovative instructional strategies and engage students while considering privacy issues. Finally, this paper discusses ways to further explore and address privacy locally and includes a comprehensive resource list for further reading.

Students' Use of and Attitudes Toward Cloud-Based Tools

A recent 2010 survey of undergraduate student use of information technology asked students what web-based services they were currently using to support their college education for any of their courses during the quarter/semester of the survey. Many learners reported use connected with instructional activities and also said that many of the tools were assigned by an instructor.

Table 1. Students Using Web-Based Technologies in Courses the Quarter/Semester of the Survey

Web-Based Technology Use in Courses	Percentage Using Technology
Web-based word processor, spreadsheet, presentation, and form applications (Google Docs, iWork, Microsoft Office Live Workspace, Zoho, etc.)	36.2%
Wikis (Wikipedia, course wiki, etc.)	33.1%
Social networking websites (Facebook, MySpace, Bebo, LinkedIn, etc.)	29.4%
Video-sharing websites (YouTube, etc.)	24.3%
Web-based calendars (Google Calendar, etc.)	17.4%
Web-based citation/bibliography tools (CiteULike, OttoBib, etc.)	17.2%
Blogs	11.6%
College study support (Cramster, Turnitin, Essay Checker, ShareNotes, etc.)	10.9%
Photo-sharing websites (Flickr, Snapfish, Picasa, etc.)	5.4%
Micro-blogs (Twitter, etc.)	4.3%
Online virtual worlds (Second Life, Forterra, etc.)	1.4%

Source: Shannon D. Smith and Judith Borreson Caruso, with an introduction by Joshua Kim, The ECAR Study of Undergraduate Students and Information Technology, 2010 *(Research Study, Vol. 6), Boulder, CO: EDUCAUSE Center for Applied Research, 2010, available from* http://www.educause.edu/ecar.

In the past decade, the technology available in the cloud and how it's used for teaching and learning have undergone a significant transformation. The first wave of the World Wide Web enabled global distribution of information for consumers. Today, with blogs, microblogs, wikis, and social networks, our focus has expanded beyond simple consumption to active production. Whereas companies dominated Web 1.0, Web 2.0 is dominated by users and communities. Whereas information was owned and controlled, accessible through portals, and categorized by formal taxonomies, it is now socialized. Information is openly shared, transparent, and democratized; it is delivered by RSS and categorized by producers and consumers alike with a folksonomy of tags. Moreover, whereas Web 1.0 was static and Web 2.0 is social, Web 3.0 will be semantic—reconnecting existing data for other artificially intelligent uses. Some call Web 3.0 the World Wide Database guided by common sense (Markoff 2006). But when common sense is driven by aggregated data about a particular student's frequently visited sites, recent searches, and posted comments or "likes" on a class wiki, a whole new realm of privacy issues emerge.

In higher education, we have seen cloud-based technologies enable a shift from faculty-driven lectures to student-driven conversation and collaboration. While this shift promotes a promising pedagogical step, it also presents new challenges for institutions whose responsibility to protect students' personal privacy has not changed.

Ease of Use and Privacy Concerns

Academic researchers, market research firms, and large foundations have conducted studies measuring attitudes and behavior toward online privacy. For example, Smith, Millberg, and Burke (2000) found four general categories of concern that people have about their privacy online:

- Collections: the vast amount of personally identifiable information that is collected and stored
- Third-Party Use: the sharing or selling of personal information to external parties for secondary uses
- Access: the security of stored data and its availability to unauthorized parties
- Errors: the adequacy of safeguards against accidental or deliberate errors

The Pew Internet & American Life Project (http://pewinternet.org/) reports that 84% of American adults are concerned that businesses and strangers will obtain information about them or their families. However, these attitudes vary considerably by "age, gender, cultural trait, degree of trust propensity, and experience with privacy technologies" (Hann et al. 2002). For example, the Pew study reveals that 67% of adults ages 50–64 are "very concerned," in comparison to 46% of adults ages 18–29. Similarly, other studies in academic settings show faculty members are more concerned about privacy than students. Variation also exists by academic department—it has been reported that students in arts and sciences, nursing, and education are more concerned than students and faculty members in business (Alexander, Jones, and Brown 1998). Still others found that university employees were most concerned about improper use of student information (Earp and Payton 2001).

FERPA in Cloud-Based Instructional Environments

At the root of many of the concerns over privacy in a digital era is the federal law that covers the ways in which educational institutions must maintain and safeguard student information.

FERPA: Applications and Interpretations

FERPA (also known as the Buckley Amendment)—sponsored by New York Senator James Buckley in order to address a number of concerns and ambiguities identified by parents, students, and academic institutions—was enacted to protect the accuracy and privacy of student records at all levels of schooling. For students in grades K–12, the rights to access and control access to records belong to the students' parents. When a child turns 18 or enrolls in an educational institution beyond high school, the rights are transferred away from the parents and afforded to students directly. When FERPA was enacted in 1974, education records consisted of information kept on paper in locations maintained by an instructor or the university registrar. The rights afforded to parents and students under FERPA were, at the time, all under the stewardship of the registrar. These rights include the right to inspect and review education records maintained by the school, to request that records be corrected if anything is incorrect or misleading, to choose not to have directory information disclosed, and to release education records only with written permission.

Today, the same rights are protected under FERPA, but since the educational (at least instructional) environment is somewhat different, institutions and faculty members are left wondering how to apply 1974 FERPA to today's increasingly digital and open educational environment, especially in areas where interpretations and requirements related to the education record are unclear.

Considering FERPA and Advancing Innovation

For the past few years, instructors have been incorporating cloud-based teaching and learning technologies into their courses, often with little or no thought about the privacy implications of having

student work in an online, sometimes open, environment. Institutions and faculty members need to be cognizant of FERPA requirements and determine how to interpret them for their classes, as well as develop ways for instructors to structure assignments in such a way that supports course objectives and innovation.

The section of FERPA that is most relevant to instruction is the part that states, "generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record" (http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html). Education records are currently defined as records that are directly related to a "student" and maintained by an "educational agency or institution" or by a party acting for the agency or institution (http://www.ed.gov/policy/gen/guid/fpco/pdf/ht12-17-08-att.pdf). When a student's work is posted online, a record of the student's work and involvement in the course is automatically created and thus may be subject to FERPA restrictions, depending on the institution's interpretation of what is "maintained" by the college or university. This is different from a conversation occurring in a face-to-face classroom, where the event is fleeting and not recorded and thus not part of an education record. Similarly, an assignment that is not submitted to the instructor or other party acting on behalf of the institution may not be subject to strict FERPA compliance since it never became part of the education record. Peer review, for example, may not fall under FERPA restrictions because the work is shared between students before it is turned into the instructor, at which point the review becomes part of a student's education record (see *Owasso ISD v. Falvo*).

It is important to note that FERPA is an obligation of the institution, not of the specific faculty member, given that case law does not provide an individual right of action. The consequence of a FERPA violation is a sanction by the Department of Education. Traditionally those sanctions have been in the form of an investigation and a warning letter to an institution found to be in violation. To date, no institution has suffered the more extreme consequence: a restriction on federal funds, including financial aid and grants. Thus, colleges and universities have cause to be vigilant about compliance. For the individual faculty member it is important to remember that he or she carries the weight of that obligation for their institution. While he or she may not be personally liable for a breach, the individual may be subject to internal sanctions within the institution if actions resulted in consequences for the school.

Institutional response and attempts to comply with FERPA, especially as they relate to instruction in online environments, vary significantly. Some are integrating online education into their FERPA training for faculty members and employees, such as the Colorado Community Colleges. They have integrated online learning scenarios into their FERPA training (http://at.ccconline.org/faculty/wiki/Policies_%26_Procedures_-_FERPA_-_Scenarios_and_Tips). Other schools have taken their policies further and created guidelines and student consent forms for faculty members to use. North Carolina State University has created a FERPA Privacy checklist for online course hosting, for example, which guides faculty members in the interpretation of FERPA in a web-based environment, while also providing examples of alternatives: http://www.ncsu.edu/general_counsel/legal_topics/ferpa/ferpa-forms/FERPA_Privacy_Checklist_for_Online_Course_Hosting.doc.

Teaching and Learning in the Cloud: Potential Solutions

Privacy in cloud-based teaching and learning environments is likely to remain a significant issue, and as the digital landscape continues to evolve, a single solution is increasingly unlikely. Institutions will undoubtedly need to approach the issue at multiple levels with varied strategies. Here, we recommend three strategies for institutions to consider: legal, policy, and guidelines; technical; and social and educational.

Potential Solutions: Legal, Policy, and Guidelines

While institutions and faculty members are required to comply with FERPA regulations, many actions can be regulated through existing or modified Codes of Honor or Codes of Conduct policies. Just as many businesses are developing and communicating social media policies to protect their brand and reputation, so too are educational institutions for their staff, faculty members, and students. For instance, the Colorado State University social media policy applies to social media accounts created by university employees for the official business purposes of the university, including Colorado State University faculty, groups, departments, programs, entities, etc. Part of their social media policy requires an application in order to use social media tools and includes various communication mediums such as Facebook, Twitter, LinkedIn, Flickr, and YouTube (http://socialmedia.colostate.edu/page/Social-Media-Policy.aspx).

Another approach taken at many institutions is the use of a student consent form that students can submit prior to participating in a public course-related site, such as a class blog or wiki. For example, the registrar at the University of Oregon and the library at North Carolina State University post consent forms for faculty members to distribute to students so they may legally consent to contribute to a blog, wiki, or other publicly available site. The policy states, "Students must provide voluntary written consent prior to their inclusion in a course blog and prior to University employees or agents disclosing (including electronic posting) any other FERPA-protected information from students" (http://www.ncsu.edu/policies/academic_affairs/library/RUL02.61.01.php).

As is evident in the examples we've included in this paper, institutional reactions vary widely and should be tempered so as to not adopt an overly restrictive approach. Some institutions, such as Cornell University (http://www.cit.cornell.edu/services/blogs/about.cfm), encourage instructors to allow students to opt out of using open or public Web 2.0 tools. Doing so reduces the amount of paperwork and administrative overhead required while demonstrating the institution's intent to comply with FERPA and educate students about their options for use of Web 2.0 tools.

Potential Solutions: Technical

Increasingly, institutions are working closely with vendors of Web 2.0 tools to implement local institutional instances of cloud-based tools, thus enabling the pedagogical benefits while protecting students' privacy behind the institutional firewall. For example, within the Graziadio Learning Environment and Network (GLEAN) at Pepperdine University, students, faculty, and staff use various multimedia and social network tools authenticated with a single sign-on using their Pepperdine user ID and password. While many of the tools within GLEAN are available to the public at large (such as Google Apps, Elluminate, VoiceThread, and Yammer), Pepperdine has licenses for internal instances of each of these tools within the Pepperdine domain. By both technical configuration and contract, Pepperdine owns and controls all contained data. In some cases, such as with Google Apps and VoiceThread, Pepperdine students may intentionally choose to share their work outside the Pepperdine domain. Yammer, on the other hand, is a social network specifically for the Pepperdine community only. Because it is used for class discussions (including evaluative feedback from professors), faculty committees, and general internal communication, all data is secured within the Pepperdine domain.

Universities that have implemented Google Apps Education Edition also enjoy domain-specific protections. As SaaS (software as a service) vendors—such as Google, VoiceThread, and Yammer—continue to expand their market reach beyond individual consumers to businesses and educational organizations (which are sensitive to data protection and privacy), technical solutions and alternatives will become increasingly available.

Potential Solutions: Social and Educational

As studies on individual's attitudes and behavior reveal, there seems to be an inconsistency between the amount of privacy desired and action taken to protect it. While it may speak to a lack of understanding, this inconsistency also highlights a culture that values and protects privacy differently from previous generations. Some institutions have taken steps to strengthen that culture, especially among students. For example, Cornell University offers guidelines encouraging students to protect their own privacy on Facebook or other tools outside class while emphasizing how the university respects and protects their privacy and employs a no-monitoring policy (http://www.cit.cornell.edu/policies/socialnetworking/facebook.cfm). Similarly, the University of British Columbia shares resources and encourages students to think about their online presence through the Digital Tattoo Project (http://digitaltattoo.ubc.ca/). Here, students produce and distribute content engaging their peers in issues of digital privacy, identity, rights, and responsibilities. Whatever the approach, it's critical to teach the value of online privacy in general, FERPA and other privacy legislation in particular, the scope and amplification of the Internet, and the construction of students' online identities, especially given the confluence of both the personal and the professional.

Getting Started at Your Institution

In this paper's brief review of institutional approaches to address privacy in cloud-based teaching and learning environments, a variety of institutional responses were found, ranging from student awareness campaigns to institutional policies prohibiting any unauthorized cloud-based tool use. It's clear that FERPA requires protection of students' privacy as it relates to their education record, but what is not clear are the components and boundaries of that record. For instance, does peer commentary or critique fall under the education record? If students sign a form consenting to participate in an open and public course-related site, have institutions met their FERPA requirements? What options or alternatives, if any, to open and public course-related environments are institutions or faculty members required to provide students?

Institutions interested in addressing some of these challenges can begin by considering some initial steps and questions to get started:

- **Form the group.** Assemble a group to begin exploring the issues and include faculty members, legal counsel, administrators, the registrar, and any others involved who might assist in devising a strategy. These individuals could also be consulted in stages as you learn more about current instructional practice at your institution.
- **Examine and understand current, local cloud-based teaching and learning practices.** It's always helpful to have some understanding of current instructional practice at your institution. This information can help to know how privacy in online and open environments is currently addressed, if at all. It can also inform the kind of response that might be most appropriate, given the circumstances: legal, policy, and guidelines; technical; social and educational; or some combination of these.
- **Review what similar institutions are doing.** Although this is an emerging area, there are many examples already of how institutions are responding at various levels.
- **Pilot a strategy.** Since this is such a quickly changing area, it might be a good idea to put something in place, try it out for a semester or two, regroup, and revise as necessary. This is something often not done, especially when new policies or guidelines are created, but can be useful in determining whether the original objectives were met.

Below are three scenarios having to do with the intersection of cloud-based teaching and learning with concerns about privacy. Following each scenario is a set of questions meant to assist institutions in beginning to identify corresponding privacy concerns and generate discussion locally around the issues identified in this paper. Some of these situations may be ones you've encountered, but examining local cloud-based instructional practices and generating additional scenarios can be helpful in exploring this topic and identifying next steps.

While faculty members—as employees of the institution that is obligated to comply with FERPA—would do well to go through these checklists and be able to demonstrate due diligence towards compliance, it is important to remember that the Department of Education understands the challenge colleges and universities face in melding old law with new technologies. The criterion is intent. A faculty member acting on behalf of the institution to promote educational missions is different from one found to have acted with reckless disregard of education records. Due diligence is not only the key to compliance but also a demonstration that the whole—educational missions—is greater than the sum of specific checklist parts.

Scenario 1

Dr. Schorr and Dr. Wood are longtime research colleagues at neighboring institutions. When they get together, they tend to share teaching stories and tips with each other. Recently, Dr. Schorr has learned of Dr. Wood's success in having her students maintain public blogs with assigned writings and reflective posts, which she grades periodically throughout the course. After considering this innovative approach, he decides to implement her method in his upcoming Fall classes. He makes sure he includes in his syllabus a few notes about protecting his students' privacy and complying with FERPA regulations. Specifically, he warns his students never to post anything about their class standing, major, or residence hall.

- Would Dr. Schorr's activities constitute a violation of FERPA?
- Is the "disclaimer" he added to his syllabus sufficient to address FERPA?
- What, if any, are Dr. Schorr's obligations in relation to privacy and the student blogs?
- What should Dr. Schorr do to determine how to proceed in this case?
- What questions might need to be asked to make a determination about compliance with FERPA?
- What is Dr. Schorr's or the institution's responsibility if a student follows Dr. Schorr's instructions to comment on each other's blogs but inadvertently divulges some of the blogger's protected information?

Scenario 2

At a departmental faculty meeting, Dr. Williamson was discussing some of the features of a local LMS with another colleague. Dr. Alem had a heavy teaching load that term, and, to help streamline his workload, he was thinking of combining two of his courses, graduate and undergraduate, into a single course site on the LMS. In both courses he assigned many of the same readings, and his plan was to simply set up two different discussion forums for each of the courses. As Dr. Williamson listened to Dr. Alem's plan, he started to think of the ramifications of students in different courses having access to each other's discussions and work.

- Would Dr. Alem's activities constitute a violation of FERPA?
- What, if any, are Dr. Alem's obligations in relation to privacy and students' discussion board contributions?

- What should Dr. Alem do to determine how to proceed in this case?
- What questions might need to be asked to make a determination about compliance with FERPA?

Scenario 3

In a graduate research-methods course, students are required to produce a proposal for their doctoral dissertation. The instructor's pedagogical approach is a highly iterative process by which students complete the proposal in stages and move through the stages when the instructor is satisfied with their progress in each. In order to avoid having students submit several documents, he asks them to set up one Google Doc to complete each stage and, ultimately, the entire proposal. Since the institution does not have a local Google Apps implementation, the instructor asks students to set up Gmail accounts and Google Docs to work on their proposals. Throughout the course, students are asked to share the doc with the instructor and other students in the course to receive feedback and finally approval to go to the next stage in the proposal-development process.

- Do the instructor's activities constitute a violation of FERPA in this situation?
- What, if any, are the instructor's obligations in relation to students' privacy?
- What if the students are only asked to share the documents with the instructor and not other students? Would that constitute a FERPA violation?
- What if a student makes the document public, but this is never disclosed or obvious to the instructor?
- What if the institution had a local instance of Google Apps? Would anything in the above scenario constitute a FERPA violation?
- What questions might need to be asked to make a determination about FERPA compliance?

Resources

The following resources delve more deeply into the questions surrounding privacy in an era of digital learning environments.

Research and Articles

- Alexander, Paulette, and Sarah Brown. "Attitudes Toward Information Privacy: Differences Among and Between Faculty and Students" (1998). AMCIS 1998 Proceedings. Paper 17: http://aisel.aisnet.org/amcis1998/17.
- Earp, Julia B., and Fay C. Payton. "Data Protection in the University Setting: Employee Perceptions of Student Privacy." Proceedings of the 34th Annual Hawaii International Conference. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=927152.
- Hann, Il-Horn, et al. "Online Information Privacy: Measuring the Cost-Benefit Trade-Off." Twenty-Third International Conference on Information Systems (15–18 December 2002): http://www.comp.nus.edu.sg/~ipng/research/privacy_icis.pdf.
- Milberg, Sandra J., H. Jeff Smith, and Sandra J. Burke. "Information Privacy: Corporate Management and National Regulation." *Organization Science* 11.1 (January–February 2000): 35–57.
- Strentz, Herb. (Drake University/School of Journalism and Mass Communication): http://www.abanet.org/publiced/focus/priv_20thcentury.html

Websites

- Family Educational Rights and Privacy Act (FERPA), Department of Education: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
- North Carolina State: FERPA in Teaching (includes consent forms, guidelines, and policy information): http://www.ncsu.edu/general_counsel/legal_topics/student_privacy.php#B.
- CCCOnline Faculty Wiki (includes FERPA tips, guidelines, and resources; see also Scenario 3): http://at.ccconline.org/faculty/wiki/Policies_%26_Procedures_-_Faculty_Handbook_-_Teaching_for_CCCOnline_-_Faculty_Role_In_the_Classroom_-_Ferpa_Training.
- NACUA Notes: FERPA (includes FERPA guidelines, examples, and resources): http://counsel.cua.edu/FERPA/publications/NACUANOTE.cfm.
- Cornell Information Privacy and Security: http://www.cit.cornell.edu/policies/infoprivacy/index.cfm.
- Northwestern University Information Technology, Policies and Guidelines: http://www.it.northwestern.edu/policies/index.html.
- Colorado State University Social Media Policy: http://socialmedia.colostate.edu/page/Social-Media-Policy.aspx.
- GLEAN—Graziadio Learning Environment and Network: http://tinyurl.com/aboutGLEAN.
- NCSU Policies, Regulations, and Rules: Use of NCSU Libraries "WolfBlogs" Service: http://www.ncsu.edu/policies/academic_affairs/library/RUL02.61.01.php.

Reports and Guideline Documents

- "Shades of Gray: How FERPA, Copyright, and Other Legal Issues Impact Technology Use in the Classroom": http://www.educause.edu/Resources/Workshop04AShadesofGrayHowFERP/196754.
- "Outsourcing and Cloud Computing for Higher Education," Tracy Mitrano, January 11, 2010: http://www.cit.cornell.edu/policies/publications/cloud/.
- "Cloud Computing Guidelines for Teaching, Administrative Support, and Research," The Ohio State University: http://cio.osu.edu/policies/ccg_V62.pdf.
- The Ohio State University, Cloud Computing Guidelines and Policies: http://cio.osu.edu/policies/cloud.html.