TCC 2013 Conference Proceedings

Informed "Privacy" and "Terms of Use" Policies for Online University Courses

Ellen R. Cohn, PhD, CCC-SLP
Department of Communication Science and Disorders
School of Health and Rehabilitation Sciences
University of Pittsburgh, Pittsburgh, Pennsylvania, 15250
United States
ecohn@pitt.edu

Valerie J.M. Watzlaf, PhD., RHIA, FAHIMA
Department of Health Information Management
School of Health and Rehabilitation Sciences
University of Pittsburgh, Pittsburgh, Pennsylvania, 15260
United States
valgeo@pitt.edu

Abstract: Before gaining access to most course management websites, university students, teaching assistants, and faculty members must first enter a user name and associated password. While log-in and authentication processes imply that a course website and the information contained therein is restricted to registered students, assigned faculty, and teaching assistants, such is not necessarily the case. Obligatory "log-in" safeguards and suggested "log-out" rituals can promote an inflated sense of the privacy and security of online courses. In reality, the elements of course privacy and security are multi-layered, with potential protections and vulnerabilities that may not be fully obvious. It is therefore important that participants in the virtual classroom appreciate the potential protections and limitations to course privacy. Such knowledge can allow students and faculty alike to make informed choices concerning their participation (e.g., the nature of the content they post; performance characteristics such as date/time of participation). This paper will describe how course-specific privacy statements can provide participants with a greater sense of "informed privacy." The authors will suggest elements for inclusion and instructor practices to minimize risk, including a requirement that all users of a course management website agree to a "Terms of Use" policy.

Introduction

To what extent is a university course website private? The response to this question will likely be variable, dependent upon the course practices and the participants therein; the university's policies, procedures, and computing systems; characteristics of the course website; the privacy practices of the course website's commercial vendor (especially

when the course is housed on their servers); the participant's Internet carrier; the behavior of the course users, and even, the access afforded to persons in the course user's environment who might be able to observe the course website. These questions further extend to the online services offered by a textbook publisher, ancillary communication technologies such as Voice over Internet Protocols (e.g., Skype; Face Time) and the use of text-messaging.

When good intentions, ethical practices, and robust privacy and security practices converge:

- Students' discussion postings (especially those that reveal personal information such as health status, political views, or proprietary information about employers or co-workers) *will not,* without their permission, find their way to Facebook, an external listserv, or a media outlet -- even years after completion of the course.
- Faculty members' recorded, posted lectures *will not* appear without their consent on YouTube.
- Posted quiz questions or an online examination harvested from a textbook publisher's test bank) *will not* be shared with students taking a similar course in another university.
- Students' course bios and introductory e-mails *will not* be retained by a third-party Internet carrier and shared with their affiliates (even in other countries).
- Faculty members *will not* access online student assignments, grades, and student PeopleSoft (or other identifying numbers) on unsecured Wi-Fi networks in hotel rooms or coffee shops, thus compromising sensitive student information.

The obligatory "log-in" and suggested "log-out" rituals associated with proprietary course websites promote an inflated sense of privacy and security -- implying that access to the course website and the information contained therein are restricted to registered students and assigned course personnel. In reality, course privacy and security are multi-layered, with a host of potential and not readily obvious vulnerabilities that extend beyond the behavior of the course participants.

Though faculty and their students enrolled in distance education classes may be obligated to engage in a virtual classroom, the practice of alerting them to the potential limitations to course privacy can allow them to make informed choices concerning the nature of their participation (e.g., the content they choose to post and performance characteristics such as date/time of participation).

This paper will describe how course-specific privacy statements can provide participants with a greater sense of "informed privacy," as well as instructor practices to minimize risk. The concerns and solutions presented herein are informed by the authors' work on the privacy and security of protected electronic health information in both traditional and telemedicine environments, as well as their experiences and that of their colleagues who have delivered online education in several universities.

Privacy Vulnerabilities in Online Courses

Student Behaviors

To encourage interaction in their online classes, faculty variously require students to view videos of recorded instructor lectures, post discussion board entries, and comment upon the postings of other students. Students may also be required to engage in small group work online, and take online quizzes and exams.

The ability of students to copy, record and/or share such information can be accomplished with greater ease, and less detection than in the traditional, in-person classroom. Unbeknownst to faculty member or student peers, students can easily allow non-class members (e.g., peers; family; media; legislators; employers; members of law enforcement) to access the current or saved content of an online course.

Of great concern, is that there is no time limit to such behavior. Students can readily copy and retain course content for later distribution. This can occur well after students receive their final course grades and degrees -- thereby evading university judicial policies and sanctions. These possibilities, though hopefully not the norm, beg consideration for "Terms of Use" policies that students complete before first entering a course website.

Faculty Behaviors

As mentioned previously, faculty members can engage in risky behaviors that compromise the privacy of students in an online course. This includes the viewing of course grades and assignments over an unsecured wireless network. It is not uncommon for a faculty member attending an academic conference to admit prolonged use of an unsecured Wi-Fi network to access their course website (e.g., because their hotel does not offer a secured option; the fee for multiple days of use is too expensive and/or unreimbursed by their university; and/or the sole option for secure access is inconveniently restricted to the hotel room).

Faculty in some courses unwisely structure assignments in such a manner that students feel compelled to reveal information in required posts to a class-wide discussion, or to their project group, that would not otherwise be posted to a public website. This includes content concerning their employment experiences, clients or patients, family members (including minors), health status, religious, and political views, and even past and current behaviors.

Third Party Security Issues

While many universities house their course web sites on their own servers, others contract with third party course management vendors to house the content. Students may also (sometimes at the instructor's suggestion), use third-party vendors outside of the university course management site to facilitate group communication.

It is important for all academic stakeholders to review these vendors' privacy policies. Given that it is a rare student who would independently seek a privacy statement to review, we recommend links to such policies in a course's "Privacy Statement."

The following articles discuss a range of concerns about the privacy and security policies of services such as Skype: Watzlaf, Moeini, & Firouzan, (2010); Watzlaf, Moeini, Matusow, & Firouzan, (2011); Cohn & Watzlaf (2011). Many of the privacy and security issues addressed in the checklists contained therein can also be applied to web-based course management systems that are the subject of this article.

To their credit (as retrieved on 12/24/2012), each of the major course management systems we surveyed posted one or more privacy policies (Table 1). However, it must be cautioned that stated good intentions do not insure that explicit policies will be upheld.

Table 1. Third Party Course Management Systems and Privacy Statements

Course Management System Exemplars	**References to Privacy Statements**
Blackboard	http://www.blackboard.com/footer/privacy-policy.aspx , and http://www.blackboard.com/Footer/Privacy-Center.aspx
Desire2Learn	http://www.desire2learn.com/contact/privacy/
Pearson eCollege	http:// ecollege.com/Privacy_Policy.learn
Moodlerooms, Inc	http://www.moodlerooms.com/privacy-policy
Agilix Labs	http://agilix.com/privacy-policy/
Open Source Classroom Exemplars	**References to Privacy Statements**
Khan Academy	http://www.khanacademy.org/about/privacy-policy
edX	https://www.edx.org/privacy
Voice Over Internet Protocol Exemplars	**References to Privacy Statements**
Skype	skype.com/go/privacy
Face Time	http://www.apple.com/privacy/

Instructor Based Preventative Tactics

Thoughtful and vigilant instructors can serve as a first line of defense against potential assaults on course privacy and security, by deploying the following safe instruction practices:

1. Anticipate and Prevent Content-Based Privacy Violations

There is inherently some degree of risk for privacy violations in both on-campus and on-line classrooms. Even after receiving stern warnings, it is difficult to ensure that a student

in an in-person classroom will not illicitly record another student or the faculty member, and subsequently post the content.

A student in a traditional, on-campus classroom might erroneously share a client's protected health information in a term paper, discuss a minor's (by name) educational status, or relate a circumstance that could compromise their own current or future employability. We expect that students might make unintentional mistakes, and hope that the classroom (and paper shredders) will provide a safe haven for such circumstances -- assuming that no future plans for criminal activity are related.

However, the online course website can be far less forgiving than the in-class environment with paper based assignments:

- If a student in the health sciences mistakenly posts a client's protected health information on an online course site, they will have likely violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, enforced by the US Office for Civil Rights.
- If a student in a business or communication curricula presents a case study that relates negative attributes of their place of employment (especially when they have indicated where they work on a statement of introduction or a posted bio), the information cannot be contained in the same manner as if presented in an oral presentation in an in-person classroom with no electronic recording.
- If a student posts an online discussion entry with errors in spelling, grammar, or unwise word usage (e.g., a highly inflammatory word), the content can easily become accessible to an audience beyond the instructor or university.

Content posted in university course management can enjoy a life-long shelf-live, especially when text or photos fall out of the control of the student and instructor. In the case of the open source EdX site, the postings may persist beyond one course cycle, and the burden of selecting an unidentifiable user name falls to the user:

> "We may provide your Postings to students who later enroll in the same classes as you, within the context of the forums, the courseware or otherwise. If we do re-post your Postings originally made to non-public portions of the Site, we will post them without your real name and e-mail (except with explicit permission), but we may use your username."
>
> "Comments or other information posted by you to our forums, wikis or other areas of the Site designed for public communications or communications among registered class members may be viewed and downloaded by others who visit the Site. For this reason, we encourage you to use discretion when deciding whether to post any information that can be used to identify you to those forums (or other public or class wide areas)." (https://www.edx.org/privacy; Retrieved 12/24/2012)

How might an online instructor engage in risk management to avoid content based privacy violations?

- Inform the class concerning potential content-based privacy violations and why students must avoid these circumstances. Institutionalize this content in a "Terms of Use" agreement that is a requirement for access to the course materials.
- Construct assignments that do not rely upon a student's need to reveal authentic, confidential content that can easily be associated with persons or organizations.
- Discuss how, as with any website, there could be unimagined privacy and security issues related to their course website that are beyond even the university's best efforts and control, and that students should therefore exercise wise judgment concerning electronically based content.

2. Manage and Disclose "Guest" Access

As a marketing strategy, some universities allow unidentified "guests" to access various parts of a course website, without logging in. In certain instances, the instructor can control the level of guess access. Instructors should be alerted to this possibility, especially when the course system's default settings allow for the presence of guests. Guests whose presence is unbeknownst to the faculty and students should never be allowed to view students' posted profiles, discussion board entries, or assignment submissions.

In some departments and universities, administrators and other staff who are not assigned to teach an online course are nonetheless granted access, ostensibly to monitor the quality of the instruction and/or to assist with technical aspects of the course. They may periodically receive statistics concerning the activity of the instructor and students, and the performance of the website. Such personnel might include departmental supervisors, administrators, graduate student assistants, and information and computing staff. This practice access begs the following questions: Is there a site usage audit process in place? What level of access are these individuals afforded (e.g., discussion boards? grade book? posted student assignments?) Are these personnel formally trained in principles of confidentiality and security? What needs precipitate such visits? Will instructors and students be proactively informed of such classroom visits, and if not, why not?

Even when these individuals visibly appear in the list of course users, their presence may rarely be realized by students or their busy instructors who do not regularly monitor the user list. Therefore, if guests can visit a course, the class should be informed of that possibility in an "Informed Privacy Statement. "It is not sufficient to assume that students or instructors might view the online class participant list. And, even if they did, observers can be added and subtracted any time of day or night, unbeknownst to both students and faculty.

An ethical operating principle is that the presence of attendees in the online classroom, should be as transparent as in an on-campus, physical classroom. No one in an online classroom should wear a "cloak of invisibility." However, if such is permitted, it should be revealed in the course's "Informed Privacy Statement." This principle is consistent with Cohn and Wilson's (2003) recommendation that faculty pre-disclose to students when non-obvious monitoring or tracking technologies may be activated in their online classroom, with the benefit of affording "an opportunity for instructors to **demonstrate**

respect for their students and to **model ethical communication."** Ethical academic communicators disclose the information needed by students to make fully informed decisions about their behavior in the online classroom.

3. Construct an "Informed Privacy Statement"

Online course websites routinely post policy statements that relate to copyright obligations, web based accessibility, access to disability services, recording of content in the (in-person) classroom) and even course continuity plans in the event of disruptions.

We recommend that universities follow the example of open source websites such as Khan Academy (http://www.khanacademy.org/about/privacy-policy) and edX (https://www.edx.org/privacy; i.e., a consortium of universities), and include an "Informed Privacy Statement" on each of their online course websites. The legal and ethical issues are sufficiently complex to form a multidisciplinary team (with representation from faculty; administration; computing/information services; legal counsel; privacy experts, etc.) to initially draft and periodically revise such policies.

The "Informed Policy Statement" might include the following elements:

- An "as required by law statement," similar to that offered by Khan Academy: **"** Khan Academy may also disclose User information if required to do so by law or in the good-faith belief that such action is necessary to comply with state and federal laws (such as U.S. Copyright law) or respond to a court order, judicial or other government subpoena…"
- A description of the disposition of course content at conclusion of the semester.
- A course's guest policy**,** including purposes, training of guests, conditions for such access, and whether their presence will be revealed to students.
- Whether and how a privacy and security breach will be revealed to faculty/students, and what has been done to remedy the breach and prevent it from occurring in the future.
- Links to the privacy policies of third parties who relate to the website or to whom the students are required to relate (e.g., course management system; textbook vendors who host test questions and ancillary materials, etc.)
- Whether a risk assessment has been performed to determine how private and secure the course site is including log in information, password protection, levels of encryption for certain material, the transmittal of information over the Internet, firewalls, antivirus software, authenticity of the site, whether the site has ever been impersonated, the role of the employees of the course site and their background in privacy and security of confidential information, and how long a student's personal profile information will be retained and how it will be used, etc.

While it is the purview of this paper to explore the specific elements of "Terms of Use" statements for online course web sites, these too appear necessary to deter the misuse of posted content, recording of site content by third parties, access to the course over unsecured networks, and admittance of persons who are not registered in the course. The "Terms of Use" policy should apply to all who access the site, not just students.

As currently constructed, "Terms of Use" policies are often difficult to read and too lengthy; most users rapidly scroll to the end of these statements and click their agreement to gain rapid access to the website. Privacy policies can be similarly difficult to read and even locate (e.g., when the policy is embedded deep within a website, or when a link to the policy appears in an extremely small font size at the very bottom of the opening page). These policies should instead be easy to access, read, and understand so that they might truly advance the knowledge of the user on privacy and security issues. Perhaps future privacy and "Terms of Use" policies might be constructed to assess readers' understanding and hypothetical application of the content in an engaging and interactive manner.

Conclusions

The elements of web-based course privacy and security are multi-layered, with potential vulnerabilities that may not be fully obvious to faculty members and students. It is therefore important that all participants in the virtual classroom appreciate the potential limitations to course privacy, and acquire protective strategies. Such knowledge can allow students and faculty to make informed choices concerning their participation (e.g., the nature of the content they choose to post; performance characteristics such as date/time of participation) and to uphold the privacy and security.

Given the seriousness of potential breaches, it is prudent that universities and their instructors collaborate to construct and post both "Privacy Policies," and "Terms of Use Policies," and that all persons who access an online course site affirm they have read and accept such policies before they are afforded access to the content of an online class.

References

Cohn, E. & Watzlaf, V., (2011). Privacy and internet-based telepractice. *Perspectives on Telepractice*, American Speech Language Hearing Association, 1:26-37; doi:10.1044/tele1.1.26.

Cohn, E. & Wilson, D. (2003). Ethics, Instructor disclosures and advanced instructional technologies. Conference on Teaching Online in Higher Education (TOHE), Indiana University-Purdue University Fort Wayne.

Watzlaf, V., Moeini, S., & Firouzan, P. (2010). VoIP for telerehabilitation: A risk analysis for privacy, security, and HIPAA compliance. *International Journal of Telerehabilitation, 2*(2), 3-14. doi: 10.5195/ijt.2010.6056

Watzlaf, V., Moeini, S, Matusow, L, & Firouzan, P. (2011). VOIP for telerehabilitation: A risk analysis for privacy, security and HIPAA compliance: Part II. *International Journal of Telerehabilitation, 3*(1), 4-10. doi: 10.5195/ijt.2011.6070