

Who Are All These People, and What Are They Doing in My Classroom?

After over a dozen years of following the literature regarding online teaching and several years of using courseware to supplement face-to-face teaching, this semester I am teaching my first fully online class—and there was a surprise. Half a dozen names of people who are not students and who were completely unknown to me showed up on the class roster. Some of those names I was able to remove from the course, but others I could not. Several weeks after raising this issue with the technology staff at my university, many of those names were still there. The fact that these “mystery” people were not in the earlier courses for which the Web site served as enrichment, in online classes of two individuals for whom I did peer teaching reviews this semester, or in the administrative Web site set up to serve multiple departmental purposes using the same courseware has made it harder to accept some of the justifications I’ve been offered for their presence in my class. (But I’d like to compliment the CIO and his staff at the University of Wisconsin–Milwaukee for their willingness to explore what is going on and to struggle with the issues I’m raising here.)

Though there have always been times when individuals who are neither students nor part of the instruction staff are present in the face-to-face classroom, not once in twenty years of teaching have I had to ask: “Who are all these people, and what are they doing in my classroom?” Why is the question worth asking? The presence in the online classroom of individuals who are not students, are not in-

involved with instruction, and are not guests invited for specific purposes raises several *potential* problems. The word *potential* is emphasized here because none of these issues have yet been problematic in my experience or in the experience of anyone with whom I’ve spoken about the

issue. But opportunities that are available are options that can ultimately be taken.

Two important potential problems are the invasion of privacy and the chilling of classroom debate.

- *Invasion of privacy.* Privacy laws restrict who has access to personal data about students and for what purposes. Yet one of the ways in which the digital classroom differs from face-to-face classes is that the virtual space combines activities that are physically separated otherwise. Most faculty members do not carry gradebooks and other personal information about students into the classroom; if they do, those materials are physically under the control of the instructor and not open to inspection by anyone else without the instructor’s knowledge and permission. In online courseware, digital student records can be maintained not only for students’ grades but for everything a student writes within the course, such as papers and chat conversations. Do any of the mystery people have illegal access to these student records maintained within the courseware? If so, are they aware of the law and their legal obligations? Should the institution be permitting this type of illegal access to data?

- *Chilling of classroom debate.* In my opinion, an even more important potential problem involves the possibility that the presence of mystery people in the online classroom could chill classroom debate; students might be fearful about who could be “listening in”

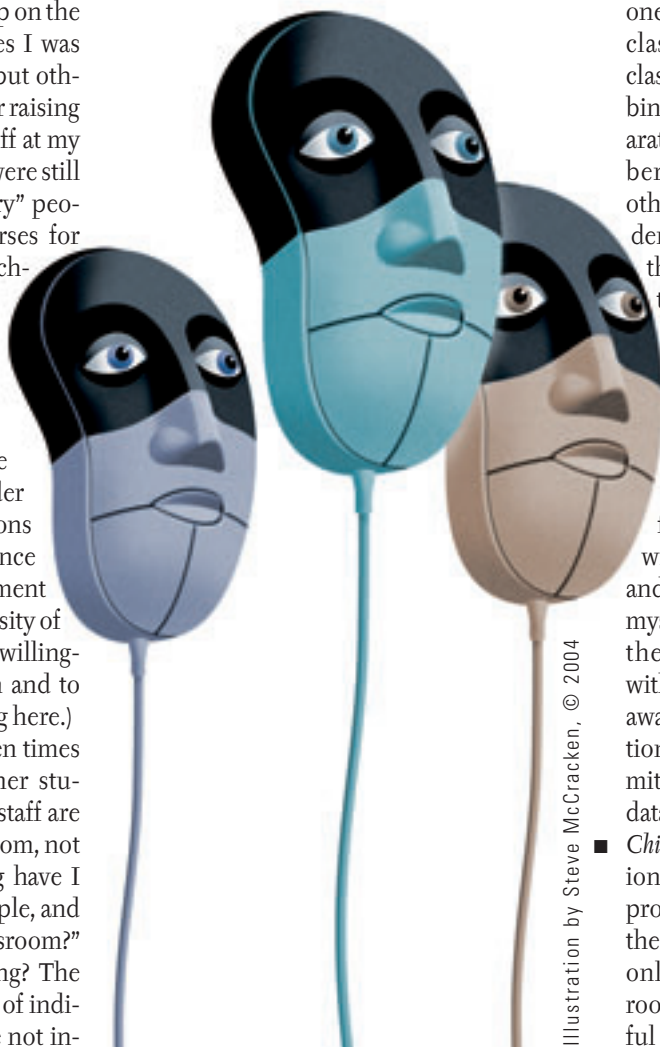


Illustration by Steve McCracken, © 2004

by reading student posts. Many of us who are passionate about teaching do so in part because the classroom is one of the few remaining U.S. spaces that operate as a public sphere. The classroom is a venue for public discussion about matters of shared concern—a place in which all perspectives are welcomed and encouraged. In the 1970s, explicit attention was directed to the requirement that professors protect the confidentiality of any conversation taking place within the classroom.¹ The concern is just as salient, if not more so, today: those responsible for the Department of Homeland Security have suggested that expressing concern over civil liberties may be suspect; a federal law requires the monitoring of courses dealing with international content; at the state level, legislation has been proposed requiring examination of the political views of public college and university faculty; and the proposed Total Information Awareness (TIA) program of society-wide informants is still a possibility. My “Human Communication and Technology” class has much more to do with new types of information work and the impact of print on Western civilization than with anything political, but this question must be raised on behalf of all of us in higher education. Constitutional law provides numerous support systems for colleges and universities that take advantage of digital technologies to significantly transform what they do and how they do it,² but constitutional protections for civil liberties still apply.

The mystery students raise other issues and potential problems. The presence of nonstudents on the course Web site could distort grade statistics (at least in my class, none of the mystery people are taking tests or doing assignments, which is dragging down average grades). Students with access to course Web sites could find answers to test questions and thus have an unfair advantage should they take online classes in the future. In addition, and significantly, there is no way of knowing if other individuals whose names do *not* appear on the class roster or

among those who can take tests are also observing the site, unobserved.

I’m told by the technical staff at my institution that there are three different groups of individuals who might show up as mystery people: (1) students working as staff at the university’s technology help desk; (2) full-time university staff; and (3) employees of the courseware company. The recommended actions for addressing the potential problems take different forms for each group:

1. *Place contractual limitations on access and use.* Employment and sales contracts provide points of leverage to protect the privacy and confidentiality of the online classroom. Employees of a software provider may request access to uses of their software, but such access need not be granted. At my university, all access by those outside the institution comes through university staff and must be justified by task-specific needs. Employment contracts with both full-time staff and part-time student staff can include provisions stating that invasion of privacy and monitoring of content for any reason are firing offenses.
2. *Place technical limitations on access and use.* Some institutions—at least some of the time—limit access to specific course Web sites for technical purposes to half an hour at a time and to the performance of a specific and specified task. Record-keeping and monitoring of such access can help ensure that this practice is consistently followed.
3. *Require privacy and confidentiality training.* Anyone who has access to student records and materials in any form should undergo privacy training that culminates in an explicit and knowing commitment to abide by privacy law. Educating staff about the importance of confidentiality must build on statutory law to include basic constitutional principles as well as ethical concerns.
4. *Provide segregated access to software for training purposes:* To ensure that help-desk staff have enough experience with courseware to be able to assist those who need help, a training-specific Web site should be set up. Such a Web site should be maintained over time as a place where help-desk

staff can experiment with different courseware features and be kept up-to-date on courseware features.

5. *Implement access processes that include the instructor:* Just as instructors are told ahead of time when service personnel will need to be in a face-to-face classroom, so they should be informed ahead of time when technical personnel need to enter a course Web site. Instructors should also be told why people are visiting the site and what they are trying to accomplish there. For any other visitor, instructors should be given an opportunity to decide whether or not the visitor is welcome during a given time period.

In sum, the concerns expressed here are in part prudential and in part a matter of appearance (a “fence around the law” to prevent even the perception that abuse might take place). They do, however, respond to the empirical and political realities of the current environment. Do I think any nonstudent cares about what we’re discussing in my undergraduate course “Human Communication and Technology” at the University of Wisconsin–Milwaukee? No. Do I believe any nonstudent has observed the class or has accessed student records inappropriately? No. But is it possible that the presence of mystery people in the online classroom might chill classroom debate or invade privacy in the future? Yes. Like software, content can be hacked, and sometimes hackers walk in the front door.

Notes

1. Wilbur J. Osborne and William I. Gorden, “A Freedom of Speech Survey of Student Opinion in a Basic Speech Course,” *Free Speech Yearbook*, vol. 9 (1970): 52–62.
2. Sandra Braman, “New Information Technologies and the Restructuring of Higher Education: The Constitutional View,” in Brian D. Loader and William H. Dutton, eds., *Digital Academe: The New Media and Institutions of Higher Education and Learning* (New York: Routledge, 2002), 268–89.

Sandra Braman is Professor of Communication at the University of Wisconsin–Milwaukee. Current work includes *Change of State: Information Policy and Power* (MIT Press, forthcoming) and the edited volume *Communication Researchers and Policy-Making* (MIT Press, 2003).

