Assessing Students Online:
Issues of Misbehaviour & Privacy

David C. Young & Wendy L. Kraglund-Gauthier

Saint Francis Xavier University

Antigonish, Nova Scotia, Canada

International Journal of Arts & Sciences' Multidisciplinary Conference
March 13-16, 2012
Las Vegas, NV

Abstract

In an educational era focused on expectations related to program accreditation, academic integrity is paramount to program success and credibility. Because Internet-based learning is not limited to geographical or political lines drawn on a map, there is a certain amount of ambiguity regarding the application of regulations and laws governing online learning and how they are enforced.

Managing the financial and accreditation needs of institutions with authentic and appropriate methods of teaching, learning, and assessment is a precarious balance – one in which the potential for misbehaving online can quickly tip the scales to the side of questioning the credibility of online learning and misusing power in terms of data privacy.

Wendy Kraglund-Gauthier and David Young explore the issue of how online students misbehave when being tested at a distance, what technological challenges emerge when verifying the identity of online students, and issues of privacy. They also include a comparison of methods used to confirm the identity of online students.

In light of the inherent challenges that emerge alongside the demand for more technology-based screening tools and devices, Kraglund-Gauthier and Young question whether solutions lie in competence-based assessment for earning, rather than a reliance on surveillance. They argue that in spite of stakeholders' best efforts and best intentions, legislation directed at ensuring online privacy is fraught with potential challenges.

The Context of Online Learning

Managing the financial and accreditation needs of institutions with authentic and appropriate methods of teaching, learning, and assessment is a precarious balance—one in which the potential for misbehaving online can quickly tip the scales to the side of questioning the credibility of online learning and misusing power in terms of data privacy.

The speed at which technologies have changed educational practices has, in some cases, moved faster than the creation and implementation of effective strategies for teaching at a distance and the authentic assessment of e-learning. For many educators and institutions of higher education, the convenience of online learning does not outweigh the challenge of monitoring the assessment of student learning, especially at a distance.

Growth in Online Learning

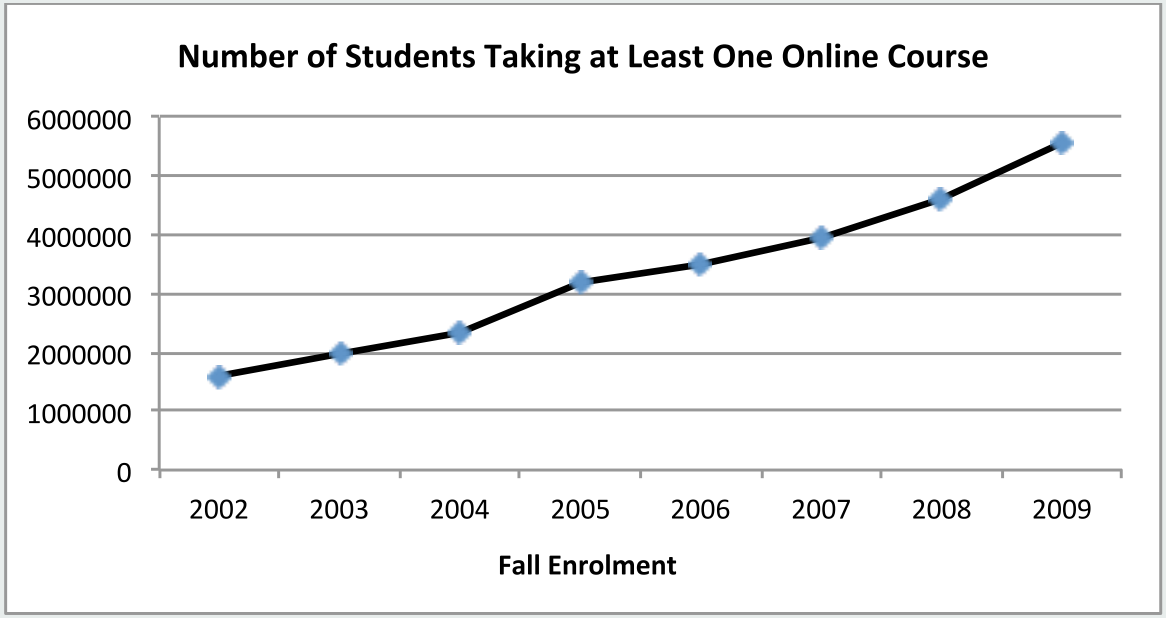

Figure 1. Total enrolment in online courses from US-based post-secondary institutions (adapted from data from Allen & Seaman, 2010, p. 8).

Rationale for Online Course Offerings

- A cost-effective way to augment their revenue bases
- A response to the changing demographics of learners
- Convenience for students
- Accepted legitimacy of online learning

Through the introduction of new technologies, universities and other learning organizations are better able to compete in a global education market and tap into alternate sources of revenue.

Resistance to online learning

E-learning advocates meet with resistance from all sides, especially from accreditors and administrators. In its research, the Canadian Council on Learning (2009) also has observed faculty resistance to e-learning. Part of this resistance stems from a loyalty and ingrained preference for face-to-face learning exchanges.

(Kraglund-Gauthier, 2011)

A great deal of resistance to e-learning as a legitimate form of post secondary credentialization has stemmed from the emergence of illegitimate course credits, diplomas, and degrees granted from so-called "diploma mills."

The concerns regarding the possibility of cheating in online courses are often based on a misplaced sense of the invulnerability of traditional assessment to any form of plagiarism. ... There is a tension between making the system accessible and easy to use for the majority of users and preventing the damage caused by those with different intentions. (Weller, 2000, p. 214)

Some business students were not opposed to cheating.

Almost three-quarters of students surveyed in one research project perceived cheating online was easier than in face-to-face classes.

(King, Guyette, & Piotrowski, 2009)

Methods used to proctor students

- Physical presence of a proctor
- password-protected Internet-based tests
- camera surveillance
- keystroke analyses
- retinal scans
- finger-printing
- Online proctoring combining elements

Remote Proctoring

Both software and hardware may be involved in authentication, which makes sure the testers are who they say they are. The technology may include:

- On-board cameras commonly found on today's laptops and more advanced USB cameras that offer wider view of the test taker and surrounding environment
- Audio monitoring via on-board or attached microphone.
- A variety of browser lockdowns, software connectivity with learning management systems (LMS) or test delivery systems (TDS).
- Software designed to compare photo identification, keystroke analysis, and biometric technologies.

Comparison of Methods

Method	Advantages	Disadvantages
- Real-time monitoring via proctors physically present	- Real-time, physical monitoring of the student's actions during a testing situation - Proctor locations tend to be at academic institutions with similar concerns over academic integrity - Communication and arrangements between institutions and proctors can be made easier by established policies and procedures - Proctor can be an additional layer of security in terms of a user login to testing materials of the student's institution - Non-invasive	- Requires physical presence of student and proctor, which may not be convenient for either - Students may incur proctoring fees - Onus is on the proctor to diligently monitor student - Course work must be sent back to the student's institution, which may take time - Geographic time zones could mean one student has written an exam before or after others, opening up the potential for questions and answers to be shared between students
- Photo Identification	- Visual confirmation of identification - Student ID card chip code can be cross-linked with course assessment material - Non-invasive	- Requires physical presence of the student and a proctor or other authorized personnel - Document can be altered - Authorized personnel may not know what an official identification card looks like in other parts of the world
- User names and passwords	- Cost effective, easily implemented - Non-intrusive - Can be easily re-set or changed - A proctor can be provided with a user name and password to input on the student's behalf	- Can be shared between users or stolen - Passwords may expire or students may forget them and be unable to access required materials

Comparison of Methods

Method	Advantages	Disadvantages
- **IP address tracking**	- Identifies the geographic location of the user - Non-invasive	- Students may not always use the same computer to do work, especially if travelling during the course - Only identifies the computer's geographic location, not the individual using the computer - IP addresses can be masked and users can route IP addresses through other servers - IP addresses are considered personal information and must be protected from misuse
- **Electronic monitoring via webcam**	- Student does not have to arrange to visit a proctoring site - Can complete the assessment in familiar surroundings - Hardware and software is relatively inexpensive	- Accrued hardware and software costs - Student must be able to operate hardware - If technical failure, student may not be able to complete the assessment when scheduled - Requires physical presence of individual to monitor Internet feed - Does not take into account time zone differences - Invasive
- **Physical biometrics (i.e., fingerprint or retinal scan, voice recognition)**	- Physiological data is unique to that user - High accuracy	- Requires specialized hardware and software - Expensive to implement - Invasive
- **Behaviourial biometrics (i.e., keystroke pattern analysis, signature patterning)**	- Relatively inexpensive to implement - High accuracy - Non-invasive	- Additional software required - Requires analysis of data, expending time - Keystroke patterns could be affected by different keyboard designs, injuries, or mental stress and fatigue

Privacy Concerns

Although “computer technology and digital media have… increased the capacity to collect, process and use personal information, [they] have also deeply challenged the dynamics surrounding personal information and privacy” (Woo, 2006, p. 953).

Privacy concerns stem from the transmission of data and storage of electronic files, this, despite the idea that “much of the data collected in educational research are of little interest to hackers” (Johnson & Christensen, 2012, p. 123).

For Weller (2002), “the concerns regarding the possibility of cheating in online courses are often based on a misplaced sense of the invulnerability of traditional assessment to any form of plagiarism. ... There is a tension between making the system accessible and easy to use for the majority of users and preventing the damage caused by those with different intentions.” (p. 124)

The idea of having a databank of fingerprints on file with a post-secondary institution’s test centre seems to impinge on a student’s right to personal privacy.

When the responsibility for ensuring privacy protocols is placed on individuals who may not receive appropriate training and follow-up, or when the department experiences high turn-over and frequent new employee orientation, the likelihood of negligent activities and security breaches may increase.

In fact, if Jortberg (2009) is correct in the bold statement that “education’s value comes from the course work and interactions during classes, ultimately expressed in a degree granted for fulfilling the requirements of a program” (p. 2), the acquisition of course-based knowledge can be expedited by instilling in students a sense of academic integrity and an ethical commitment to the educational process.

Addressing Issues of Academic Integrity

- The task of creating and maintaining a culture of integrity rests with all stakeholders—each of whom bear certain responsibilities to each other and to themselves.

- Requires a concerted effort, one in which the triad of administrators, faculty members, and students each assume responsibility for "policing (catching and punishing cheaters), prevention (designing courses and assignments that discourage cheating), and virtue (creating learning communities in which students do not want to cheat)" (McNabb & Olt, 2011).

- Part of the solution lays with instructors themselves; it is imperative they are consistent and clear in their communication and administration of procedures related to their institutions' policies of academic integrity.

Addressing Issues of Academic Integrity

- Stress the importance of effectively integrating theory and practice in educational pursuits.

- In the potential immediacy of the online classroom, participants can "have multiple and ongoing opportunities to make connections between what they learn in their courses and what they do in [the world outside the virtual classroom]" (Dell et al., p. 609).

- When culminating e-learning testing measures are designed in ways which require students to synthesize materials and make connections with and beyond course content, to reflect students' experiences throughout the duration of the course, an individual hired to take the final test in place of the dishonest student is unlikely to do well.

- This necessitates a shift in educational paradigms (Mateo &Sangrà, 2007).

- The sheer growth of e-learning opportunities in the United States, Canada, and across the globe is perhaps daunting, yet that growth and enthusiasm needs to be tempered with realism and pragmatics.

- There are no indications that an e-learning enrolment plateau has been reached.

- The question is not whether organizations will offer e-learning opportunities, but rather, whether they will take the time to do it well (Rosenberg, 2001, p. xvi) and to implement effective policies and procedures that will not only guide and protect online content and interaction, but also respect their students' rights to privacy.

References

Allen, I. E., & Seaman, J. (2007). *Online nation: Five years of growth in online learning.* Needham, MA: Sloan-C. Retrieved June 28, 2011, from http://sloanconsortium.org/publications/survey/pdf /online_nation.pdf

Dell, C. A., Hobbs, S. F., & Miller, K. (2008). Effective online teacher preparation: Lessons learned. *MERLOT Journal of Online Learning and Teaching, 4*(4), 602–610.

Johnson, B., & Christensen, L. (2012). Chapter 5: Research ethics. In *Educational research: quantitative, qualitative, and mixed methods* (pp. 97–128). Los Angeles, CA: Sage.

Jortberg, M. (2009). *Methods to verify the identity of distance learning students.* Acxiom White Paper. Retrieved June 3, 2011, from http://www.acxiom.com/SiteCollectionDocuments/website-resources/pdf/White_Papers/AC-0031-09_DistanceLearningStudentsWP.pdf

King, C. G., Guyette, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *The Journal of Educators Online, 6*(1). Retrieved from http://www.thejeo.com/Archives/Volume6Number1/Kingetalpaper.pdf

Kraglund-Gauthier, W. L., & Young, D. C. (2012). Chapter 17. Will the real "John Doe" stand up? Verifying the identity of online students. In C. Wankel & L. Wankel (Eds.), *Misbehavior online in higher education.* (*Cutting-edge technologies in higher education,* Vol. 3, pp. 355–377). Bingley, UK: Emerald.

Kraglund-Gauthier, W. L. (2011). Chapter 8. Transitioning from F2F to online instruction: Putting the action into online research. In J. Salmons (Ed.), *Cases in Online Interview Research* (pp. 219–238). Newbury Park, CA: Sage.

Mateo, J., & Sangrà, A. (2007). Designing online learning assessment through alternative approaches: Facing the concerns. *European Journal of Open, Distance, and E-Learning.* Retrieved February 20, 2011, from http://www.eurodl.org/materials/contrib/2007/Mateo_Sangra.pdf

Rosenberg, M. J. (2001). *E-learning: Strategies for delivering knowledge in the digital age.* New York, NY: McGraw-Hill.

Weller, M. (2002). Chapter 8: Assessment. In *Delivering learning on the net: The why, what, & how of online education* (pp. 116–129). London, UK: Kogan Page.

Woo, J. (2006). The right not to be identified: Privacy and anonymity in the interactive media environment. *New Media & Society, 8*(6), 949–967.