An Update on Student Authentication: Implementation in Context

Lori McNabb
THE UNIVERSITY OF TEXAS AT AUSTIN

The Higher Education Opportunity Act of 2008 (HEOA) requires accreditors to ensure that an institution that offers distance or correspondence education has a process in place to establish that a student who registers in a course or program is also the same student who participates in and receives credit for the course or program. This requirement has generated a robust dialogue about academic integrity in the distance education community and has created opportunities for companies to provide student authentication technology. The Department of Education's regulation for accreditors went into effect in July 2010, providing distance educators with information on which to act in anticipation of meeting accreditor's expectations.

DEPARTMENT OF EDUCATION AUTHENTICATION REGULATION

The amendatory language adopted through the Department of Education's negotiated rulemaking process provides a specific set of ways by which to ensure a student's identity, as well as some guidelines for implementing a student authentication program (US Department of Education). These apply to both online and correspondence courses.

An accreditor must require institutions to verify students' identities through secure logins and passwords, proctored tests, or "new identification technologies and practices as they become widely accepted" (Institutional

Eligibility Under the Higher Education Act of 1965, as Amended, and the Secretary's Recognition of Accrediting Agencies). Accreditors must also inform schools that their authentication processes should protect students' privacy, and ensure that students are notified at the time of enrollment if they will incur an expense for authentication.

STUDENT AUTHENTICATION AND ACADEMIC INTEGRITY

The HEOA requirements are aimed at limiting academic dishonesty, which is a concern in all of higher education (Center for Academic Integrity, 1999; Davis, Drinan, and Bertram Gallant; Bertram Gallant, McCabe; McCabe, Treviño, and Butterfield). The body of literature on student cheating in online courses is limited, but growing. What has been published indicates that cheating is as much—but not necessarily more—of a problem in distance education than in traditional higher education (Davis et al.; Grijalva, Nowell, and Kerkvliet; Spaulding; Stuber-McEwen, Wiseley, and Hoggatt; Vilic and Cini; Watson and Sottile).

Bertram Gallant synthesized expectations in multiple fields to define academic dishonesty as plagiarism, fabrication, falsification, misrepresentation, or misbehavior. The authentication requirement in the HEOA is aimed at misrepresentation, defined as, "falsely representing oneself, efforts, or abilities" (11).

Davis et al. propose a framework of short- and long-term deterrents to academic dishonesty. Short-term deterrents stop cheating when it is happening. Long-term deterrents—which they recommend be an institution's priority—produce a culture of integrity through moral development programs and the creation of an institution-wide culture of integrity. Student authentication efforts are an example of a short-term deterrent.

Similarly, Hinman proposed that a campus engage in three simultaneous academic integrity efforts: virtue, prevention, and policing approaches. This framework has been recommended for distance education (Howlett and Hewett; McNabb and Olmstead; Olt). Authentication methods can be preventative or policing measures.

Hinman's "virtue" approach aims at creating an ethical learning community within which students want to do their own work. Some examples of ways to implement the approach in online courses, departments, and institutions are:

1. Provide information on academic integrity in the online student orientation.
2. Ask students to reflect on academic integrity in the course discussion board.
3. Lead an activity to develop a shared honor code and then ask students to commit to it.
4. Include information on academic integrity in the faculty handbook, professional development opportunities, and resources made available to faculty members online (WCET, UT TeleCampus and Instructional Technology Council).

The "prevention" approach creates barriers to student cheating through assignment design or awareness programs (Hinman). WCET et al. provide some examples of implementation: The policing approach is an effort to catch and punish cheaters (Hinman). Many policing activities also have a preventative effect. Some examples from WCET et al. of ways to implement the policing approach are:

1. Require students to share key learning from references for a paper or self-reflect on an assignment on a discussion board.
2. When grading written work, check references, comparing quotes with cited sources. Also, look for problems with the writing, such as changes in tense, multiple writing styles or varying quality of writing, references to past events as current, and older sources when new research is available.
3. Keep an up-to-date, printed copy of the course grade book in a secure place for comparison to the online version.
4. Demonstrate an institutional commitment to enforcing academic integrity policies by encouraging faculty members to report every suspected violation, acting on every report, and providing support for faculty and staff members who are handling academic dishonesty cases.

To determine what academic integrity efforts best fit the needs of a distance education course or program, it is helpful to determine if and how students are cheating. A survey of students and faculty members can help, and one is available for purchase from the Center for Academic Integrity (n.d.).

MEETING THE AUTHENTICATION REQUIREMENT

In early 2009, Eduventures released the results of a member survey on reactions to the authentication legislation. Ninety percent of respondents indicated their institution had made concerted efforts to raise awareness of integrity issues among online students, and 61 percent said that academic integrity was a priority for their distance-learning program. Almost 30 percent of the survey respondents indicated they had or would be taking steps to meet the HEOA requirements, but more than 60 percent were unsure as to whether their institutions would make policy changes.

Aceves and Aceves strongly recommend faculty involvement in decisions regarding authentication methods. Through a survey of primarily faculty members, Shaefer, Barta, and Pavone found that most respondents' institutions depend on login credentials for authentication, and just over half also used proctoring. While about half of the survey respondents believed that their current authentication method was adequate to meet the requirement, more than half said their methods needed to improve. Survey respondents also indicated that instructors, staff members, and administrators should share responsibility for student authentication, and they recommended that authentication methods be embedded in the learning management system.

Secure login and pass code

EDUCAUSE included identity / access management in its annual list of the top ten issues of strategic importance to higher education technology leaders, stating, "strategies should be based on emerging standards and best practices," and recommending ongoing review of credentialing processes (Ingerman, Yang, and The 2010 EDUCAUSE Current Issues Committee, 52). An institution may be meeting the authentication requirement currently through secure login and passcode. Nevertheless, this may be an opportune time to review policies and procedures, and update the corresponding documentation. Because of ever-changing standards, most institutions should integrate distance education security procedures with those of the overall campus.

Additionally, efforts can be made to create awareness among faculty and staff members about the connection between login security and academic integrity. For example, communications about required annual password changes can include information about the importance of limiting access to accounts and data to ensure academic integrity, and professional development programs for staff members with high-level system access can include discussions on the ethical use of that access.

Proctoring

Implementation of a proctoring program is a pedagogical decision; a decision to assess through proctored tests is a decision not to assess by other means. It is important that decisions related to the use of proctoring include input from faculty members and academic leaders.

Institutions using proctoring have a range of options available to them, from low- to high-tech. Traditional proctoring continues to be a viable option. Campus testing centers provide support for both written and computerized exams. For most subjects, tests can be made available to a distance-education student through the learning-management system, and the proctor uses a faculty-provided password to provide student access. To ensure security of the proctoring environment, it is best for students to use a testing center at an accredited institution whenever possible.

Digital proctoring (or "monitoring") at a distance is also an option, as several services are available that provide live monitoring of a student through a webcam. Many companies offering digital proctoring provide a range of security levels, including add-ons such as a lock-down browser or the ability to require a student to be authenticated through challenge questions or biometrics to access a test.

Authentication technologies

Authentication technologies are used to verify an identity claim that the student is indeed who he or she claims to be. Downes describes two ways in which to do so: the testimony of a third party to the truth of the claim, and the presentation of an artifact unique to the person that also attests to the truth of the claim.

The use of challenge questions, whereby students must answer personal questions about themselves (e.g., items related to their credit history), is an example of Downes' first category and is typically considered a verification technique. Fingerprints (anatomical biometrics) or the use of a mouse or a keyboard (behavioral biometrics) are examples of Downes' second category, and are typically considered authentication techniques. Monitoring, verification, and authentication technologies are all considered authentication technologies for the purpose of meeting the DOE requirement.

Authentication technologies currently being marketed for distance education require a student to provide information or behave in a way that matches an existing profile. Some, such as challenge questions, compare the student user to data created elsewhere, not as a part of the educational process. Others, such as mouse and typing characteristics, compare the student to a profile created on behalf of the institution. Additionally, some biometric systems match a student user with the profile once (such as at login) or periodically, and others continuously gather data on students.

When considering implementing authentication technologies, issues common to most technology implementations apply (such as how users will get help), and new ones arise. The fit between the program or campus and the type of technology used (monitoring, verification, or authentication) is a critical concern that calls for an inclusive decision-making process. The method of authentication must fit with the institution's philosophy and mission, the program's structure, and the common assessment methods used by faculty members.

A number of policy issues arise when implementing any new authentication process. For example, regardless of the authentication method implemented, an infrastructure is required to support the students and faculty members using it. Nevertheless, authentication technologies bring a host of unique policy decisions, and little guidance is available through the legislation or DOE regulation. For example:

Will the technology be used as a preventative approach, controlling student access to course items? Or will the technology be used as a policing approach, gathering data on student behaviors?

When will a student's initial profile be created—as a part of the application process, when admitted, with a financial aid application, when enrolled in an online course, or when first accessing the learning management system, or other?

How frequently will a student be authenticated? Is the frequency a set number of times based on the number of courses in which a student is enrolled, the number of times a student takes a specific action (e.g., logging into a learning management system), or some other criterion?

When will a student be authenticated—logging in to the learning management system, participating in a discussion board, accessing an assessment item, or another situation?

How will the data gathered by the authentication technology be used in the disciplinary process? Who will determine the meaning of the data gathered on a student? On what basis will cheating be determined?

Issues related to technology integration will also need to be addressed. For example, if only students in fully online courses will be authenticated, but both online and hybrid courses are in the learning management system, there has to be a process in place to identify fully online courses and assign the use of the technology to just those courses.

Student privacy and notification of expense

It is important to keep in mind that the DOE regulation also requires students' privacy be ensured. Students must also be notified at the time of registration if they will incur an expense for authentication. Whichever authentication method is used, the privacy requirement will need to be considered. Proctoring or authentication technologies may create a cost that is passed onto students, leading to the need to notify students of an anticipated expense; in most cases, the notification requirement can be met through a statement in the course description.

LOOKING TO THE FUTURE

A recent communication from regional accreditors indicates they will not stress the use authentication technologies in the near term. In a "letter from the chair of the Council of Regional Accrediting Commissions about new federal regulations impacting distance education programs" published on the WCET website, Belle Wheelan, president of the Southern Association of Colleges and Schools states:

> I'm sure one concern of WCET's readership is the rule that evolved during the first set of negotiations which requires institutions that offer courses or programs through distance education or correspondence education to have processes in place that verify or authenticate that the student who registers in such a course or program is the same student who participates in and completes the course or program and who receives the academic credit.

Accreditors are required to ensure that institutions use, at minimum, a secure login and pass code or proctored exam and, as they become available and widely accepted, new identification technologies and practices. Additionally, whatever strategies of authentication are used must protect student privacy, and institutions must notify students, before they enroll, of any additional costs that they might incur because of this verification. The Council of Regional Accrediting Commissions (C-RAC) is going to depend heavily upon the members of WCET and other distance-learning experts to keep us apprised of new technology as it becomes available.

Regardless, interest in academic integrity and student authentication on the part of accreditors is clear, and representatives of accreditors have voiced serious concerns about misrepresentation in distance education. *The Chronicle of Higher Education* recently published an article online about financial aid fraud through misrepresentation in an online education program. The article generated many comments on the site, including one by Barbara Beno, President of the Accrediting Commission for Community and Junior Colleges:

> In addition to the financial aid fraud described in this article, there is a significant issue of institutional integrity. If a "fake" student can sign up for credits so readily, can a "fake" student also "earn" credits easily? Arguing that there can be fraudulent practices in large lecture courses, and that distance education should not be required to institute more security than is presently required, is not wise if the higher education community wishes to encourage public confidence in online education. All higher education institutions need to work to ensure the quality and integrity of ALL of their forms of educational delivery systems. Without necessary oversight to ensure integrity and quality, the greater "access" provided through distance education may result in a substandard reputation for the institutions and the students who complete on-line programs and courses.

There is also evidence that regional accreditors are eager to see institutions implement broad academic integrity programs, in addition to authentication efforts. The New England Association of Schools and Colleges Commission on Institutions of Higher Education recently posted "nine hallmarks of quality for distance education." One of the hallmarks is that the instititio ensure the integrity of its online learning environments, and the four examples provided are the legislated authentication requirement, explicit references to online learning in the institution's academic integrity policies, discussion of academic integrity in orientations for online learners, and training for faculty members who teach online.

These guidelines reflect Davis et al.'s long-term deterrents and Hinman's "virtue" approach. They are also point toward the report of the Center for Academic Integrity on the fundamental values of academic integrity, which describes a community of integrity as comprised of all members of an institution (students, faculty, staff, and administrators), and built upon the shared values of honesty, trust, respect, fairness, and responsibility.

CONCLUSION

Authentication efforts should meet the needs of the institution, and its faculty members and students teaching and learning online. Most importantly, authentication efforts should be integrated into the institution's academic integrity program.

To meet the authentication requirement and to build an academic integrity program, proactive partnerships should be created on campus with faculty members, academic leaders, staff members in the office of the dean of students (or other department responsible for the academic integrity program), IT staff members, and campus administrators responsible for accreditation issues.

Staff charged with the management of a distance education program should continue to participate in the dialogue about authentication within the distance education community, sharing issues and solutions related to academic integrity in virtual learning environments. The ongoing effort will allow campuses to meet the legislated authentication requirements, and to go beyond them to create ethical learning communities.

REFERENCES

Aceves, Patricia A. and Robert I. Aceves. (2009, Fall). "Student Identity and Authentication in Distance Education. *Continuing Higher Education Review* 73 Fall (2009): 143-152. Print.

Beno, B. "Online Scheme Highlights Fears About Distance-Education Fraud." Forum message. *The Chronicle of Higher Education* 14 Jan. 2010. Web.

Bertram Gallant, Tricia. "Academic Integrity in the Twenty-First Century: A Teaching and Learning Imperative ." Monograph. *ASHE Higher Education Report* 33.5 (2008). Print.

"Best Practice Strategies to Promote Academic Integrity in Online Education." *WCET*. Western Cooperative for Educational Telecommunications (WCET), UT TeleCampus of the University of Texas System, and the Instructional Technology Council Jun. 2009. Web.

Davis, Stephen F., Patrick F. Drinan, and Tricia Bertram Gallant. *Cheating in School: What We Know and What We Can Do*. Malden, MA: Wiley-Blackwell, 2009. Print.

Downes, Stephen. "Authentication and Identification." *International Journal of Instructional Technology and Distance Learning* Oct. 2005. Web.

Eduventures. *Academic Integrity and Student Identity Validation in Distance Learning Environments* Feb. 2009. Catalog No. 66OHEQA0209. Print.

Grijalva, Therese C., Clifford Nowell, and Joe Kerkvliet. "Academic Honesty and Online Courses." *College Student Journal* 40.1 (2006): 180-185. Print.

"Guidelines for the Evaluation of Distance Education (On-line Learning)." *New England Association of Schools and Colleges Commission on Institutions of Higher Education*. Council of Regional Accrediting Commissions (C-RAC) 2009: NEASC/CIHE No. Pp90. Web.

Hinman, L. M. "Academic Integrity and the World Wide Web." *Computers and Society* 32.1 (2002): 33-43. Print.

Howlett, Bernadette and Beverly Hewett. "Securing and Proctoring Online Tests." *Online Assessments and Measurement*. Eds. Mary Hricko and Scott L. Howell. Hershey, PA: Information Science, 2006. 300-329. Print.

Ingerman, Bret. L., Catherine Yang, and The 2010 EDUCAUSE Current Issues Committee. "Top-Ten IT Issues 2010." *EDUCAUSE Review* 45.3 (2010): 46-60, 52-53. Print.

McCabe, Donald L. "Cheating Among College and University Students: A North American Perspective." *International Journal of Educational Integrity* 1.1 (2005). *Open Journal Systems*. Web.

---., Linda Klebe Treviño, and Kenneth D. Butterfield. "Cheating in Academic Institutions: A Decade of Research." *Ethics and Behavior* 11.3 (2001): 219-232. Print.

McNabb, Lori and Alicia Olmstead. "Communities of Integrity in Online Courses: Faculty Member Beliefs and Strategies." *MERLOT Journal of Online Learning and Teaching* 5.10 (2009): 208-221. Web.

Olt, Melissa R. "Ethics and Distance Education: Strategies for Minimizing Academic Dishonesty in Online Assessment." *Online Journal of Distance Learning Administration* 5.3 (2002). Web.

Schaefer, Thomas, Marguerite Barta, and Therese Pavone. "Student Identity Verification and the Higher Education Opportunity Act: A Faculty Perspective." *International Journal of Instructional Technology and Distance Education* 6.8 (2009). Web.

Spaulding, Michael. "Perceptions of Academic Honesty in Online vs. Face-to-Face Classrooms." *Journal of Interactive Online Learning* 8.3 (2009): 183-198. Web.

Stuber-McEwen, Donna, Phillip Wiseley, and Susan Hoggatt. "Point, Click, and Cheat: Frequency and Type of Academic Dishonesty in the Virtual Classroom." *Online Journal of Distance Learning Administration* 7.3 (2009). Web.

"The Center for Academic Integrity Assessment Guide*." Clemson University*. Rutland Institute for Ethics 2010. Web. 13. Jun. 2010.

The Fundamental Values of Academic Integrity. Durham, NC: The Center for Academic Integrity, 1999. Print.

US Cong. Senate. *Higher Education Opportunity Act*. 110th Cong., 2nd sess. To amend and extend the Higher Education Act of 1965, and for other purposes. *US Government Printing Office* 14 Aug. 2008. Web.

US Dept. of Education. Office of Postsecondary Education. "Institutional Eligibility Under the Higher Education Act of 1965, as Amended, and the Secretary's Recognition of Accrediting Agencies." 34 CFR 602.17. *US Government Printing Office*. 27 Oct. 2009. Web.

---. Office of Elementary and Secondary Education. "High School Equivalency Program and College Assistance Migrant Program, the Federal TRIO Programs, and Gaining Early Awareness and Readiness for Undergraduate Program Notice of Proposed Rulemaking." Federal Register 23 Mar. 2010: 13813-13907. Web.

Vilic, Boris and Mary A. Cini. "User Authentication and Academic Integrity in Online Assessment." *Online Assessments and Measurement*. Eds. Mary Hricko and Scott L. Howell. Hershey, PA: Information Science, 2006. 341-359. Print.

Watson, George and James Sottile. "Cheating in the Digital Age: Do Students Cheat More in Online Courses?" *Online Journal of Distance Learning Administration* 13.1 (2010). Web.

Wheelan, Belle S. "New Federal Regulations Impacting Distance Education Programs." The Council of Regional Accrediting Commissions. Letter. *Frontiers: The WCET Newsletter* Feb. Web. 17 Feb. 2010.