3-2017

Online Learning Integrity Approaches: Current Practices and Future Solutions

Anita Lee-Post
University of Kentucky, Anita.Lee-Post@uky.edu

Holly Hapke
University of Kentucky, JHAPK2@uky.edu

Online Learning Integrity Approaches: Current Practices and Future Solutions

Anita Lee-Post and Holly Hapke
University of Kentucky

Abstract

The primary objective of this paper is to help institutions respond to the stipulation of the Higher Education Opportunity Act of 2008 by adopting cost-effective academic integrity solutions without compromising the convenience and flexibility of online learning. Current user authentication solutions such as user ID and password, security questions, voice recognition, or fingerprint identification are not infallible and may violate students' rights to privacy or cause undue interruptions to their efforts in performing assessment tasks. Existing authentication solutions are evaluated for their cost effectiveness in preventing fraud and cheating while ensuring learner identity and honesty. Emerging technologies in the form of biometrics, surveillance systems and predictive analytics are also examined to provide insights into the future of e-authentication for ensuring the academic integrity of online learning.

Keywords: academic integrity, online education, authentication, higher education opportunity act, academic misconduct

Lee-Post, A. & Hapke, H (2017). Online learning integrity approaches: Current practices and future solutions, *Online Learning 21*(1),135-145. doi: 10.24059/olj.v21i1.843

Introduction

The number of students taking at least one online course has been growing at a rate faster than that of the overall higher education student body since 2003, reaching over seven million in 2013 (Allen & Seaman, 2015). Students enjoy the flexibility to learn anywhere, anytime, and anyplace at their own convenience and preference. On the other hand, online education gives higher education institutions a means to increase student access with the potential to reduce costs and increase productivity. Despite the growing popularity and acceptance of online education, there is concern about its rigor and quality. A 2013 Gallup poll survey found that 49% of Americans believed that employers did not perceive an online degree as positively as a traditional one. In addition, 45% of Americans thought online education provided less rigorous

testing and grading that could be trusted than the traditional classroom-based counterpart (Saad, Busteed, & Ogisi, 2013). To determine if our students' perception of academic integrity corresponded, we administered a survey to juniors and seniors in an online undergraduate course in Operations Management (n=167). We found that while nearly all students indicated they have not had someone else take an exam for them, over 45% regarded cheating in an online class as easy and 30% would cheat if given an opportunity.

There, we felt a need to address the lack of trust in online education, and an examination of its academic integrity solutions was in order. A review of current and emerging approaches to online learning integrity will be presented in this paper. The effectiveness of these approaches will then be assessed to provide insights into best practices and future solutions that may ensure the academic integrity of online learning. Here we use the term approach to denote a broad category or strategy. A specific implementation of an approach is called a solution or practice.

Background

Academic integrity is defined as a commitment to six core values, namely, honesty, trust, fairness, respect, responsibility, and courage, in all aspects of scholarly practices, even in the face of adversity (Fishman, 2012). The six core values serve to guide behavior that is congruent with the values. An investigation of the extent of academic integrity is being practiced in online education should therefore involve an examination of the values and behaviors of the institution, faculty, and students against a set standard. However, the broad nature of such investigation is beyond the scope of this paper. Thus, we narrow our focus to the institution level and adopt the Higher Education Opportunity Act of 2008 as the minimum standard against which approaches to online learning integrity are assessed.

The Higher Education Opportunity Act (2008) states that "Institutions that offer distance education must have processes through which the institution establishes that the student who registers in a distance education or correspondence education course or program is the same student who participates in and completes the program and receives academic credit." While the Act does not reflect all six core values of academic integrity, it asks institutions to provide assurance that a process is in place to authenticate learners in a virtual environment to ensure a registered student is the one who is actually doing the course work. This implies that institutions need to have a way to (1) create and maintain a virtual learning environment that only registered learners can access; (2) monitor and track registered learners' learning activities; (3) detect and deter academic integrity misconduct in general, and impersonation, in particular. Simply put, institutions are to put in place effective learner authentication solutions to prevent fraud and cheating while ensuring learner identity and honesty.

Literature Review

We conducted a literature review with the goal of identifying relevant research articles on online learning integrity solutions. Keywords including "online education," "online learning," "cheating," "academic dishonesty," "academic integrity," "authentication," "Higher Education Opportunity Act," "technology," and "technological solution" were used to search the Google Scholar, Academic Search Complete, Web of Science, and ERIC databases. Articles that were not from academic peer-reviewed outlets (e.g., periodicals, blogs) were excluded, resulting in twenty key articles. Relevant articles cited by the key articles are included to give a final set of

34 papers that form the basis of our discussion on current and future solutions for online learning integrity.

Existing online learning integrity approaches can be divided broadly into two types: prevention and enforcement. Prevention approaches are proactive strategies that stop misconduct from happening in the first place. Jones (2009) advocates the use of an honor code and authenticity statement to ensure students understand and commit to institutional values of character and integrity. The honor code provides a clear definition of academic integrity and the consequences of non-compliance, whereas an authenticity statement is a signed declaration from students acknowledging that the work is genuinely their own. In an online environment, students can be reminded of the honor code periodically and/or required to submit an authenticity statement when submitting the course work. Mcallister and Watkins (2012) suggest seven ways that an online course can be redesigned to develop students' self-regulation skills to refrain from engaging in academic misconduct. Their seven course design recommendations are: (1) use extensive calendaring to promote task planning and time management; (2) monitor ongoing stream of work instead of exams; (3) randomize exam questions to individualize an exam for each student; (4) discuss academic integrity to create awareness and commitment; (5) allow asynchronous learning to decouple student progress; (6) track student submissions to identify potential inconsistencies; (7) provide prompt feedback to facilitate a student's assessment of progress.

These prevention approaches are supported by the cognitive development theory which posits that the knowledge of academic integrity will compel an individual to act accordingly (Kohlberg, 1984). These approaches are also in line with the view of Chickering and Reese (1993) that integrity is one of the seven developmental tasks for optimal student growth and success. For the prevention approaches to be effective, an institutional culture of academic integrity needs to be developed. It requires an institution to (1) articulate clearly what constitutes academic integrity; (2) gain faculty commitment to honor and enforce integrity practices; (3) develop students' integrity and self-regulation skills; (4) develop an academic integrity system to measure, monitor, and track academic integrity development.

Enforcement approaches, on the other hand, are defensive strategies that detect academic misconduct. Software such as TurnItIn can be used to detect plagiarism for written assignments and class discussion (Heckler, 2013; Moten et al., 2013). Browser lock-down software such as Respondus can be used to control a testing environment that prevents students from printing, copying, screen-sharing, screen-capturing, going to another website, or accessing other applications while taking a test (Sewell et al., 2010). In addition, authentication solutions can be used to confirm the identity, authenticity, and presence of a student engaging in online learning activities. Authentication solutions range from the basic user ID and password to biometric schemes to video monitoring.

The first line of defense in user authentication is to allow only registered users to access the online learning systems. This is usually done by confirming the identity of the user based on the user's knowledge of unique facts about himself or herself. A user ID and password scheme is the most commonly used knowledge-based authentication solution. Other knowledge-based

authentication solutions include challenging or security questions (Ullah et al., 2012; McNabb, 2010).

While knowledge-based authentication solutions are simple and easy to use, they cannot prevent collusion and impersonation. A strong authentication solution uses the user's biometrics (who the user is or what the user does distinctively) such as fingerprint, face, iris, voice, signature, and keystroke to confirm both the identity and authenticity of the user (i.e., it is really you?) (Rabuzin et al., 2006). However, biometric-based authentication solutions require the use of special devices to read and match a user's characteristics. There are also concerns about data security and privacy issues in dealing with sensitive data on users. In addition, user characteristics such as face, signature, and keystroke require complex technology and training overhead.

Biometric-based authentication solutions can only prevent impersonation at initial login. To ensure that the user stays put after the initial login, a next level of solution called continuous or presence authentication is needed. Presence authentication solutions are of particular relevance in authenticating users taking online examinations. Video monitoring and/or recording via webcam is a commonly used presence authentication solution (Apampa et al., 2010). Once again, additional devices for video recording and sophisticated software for analyzing video footage are needed. In addition, institutions need to have data security and privacy control measures in place to safeguard sensitive user-specific data from being stolen or lost.

Another presence authentication solution is proctoring. Both face-to-face and virtual proctoring can be viable solutions to authenticating users taking high stakes examinations. Face-to-face proctoring requires students to physically go to a testing center to take a test at a specific time (Larson & Sung, 2009; Shapley, 2000). Virtual proctoring usually is arranged with a third-party provider such as ProctorU (www.proctoru.com), RemoteProctor (www.remoteproctor.com), and SmarterProctoring (www.smarterprocoring.com) (Dunn et al., 2010). Depending on the level of authentication solutions needed, it costs from less than $10 to over $100 for each proctored examination. For example, RemoteProctor charges an annual fee of $30 and an equipment fee of $125 to use fingerprints for student identification, and video surveillance and recording systems for continuous authentication (Rodchua et al., 2011).

Assessment of existing approaches

In tables 1 and 2 we evaluate the online learning integrity approaches for their cost effectiveness with respect to the stipulation of the Higher Education Opportunity Act. Costs from the perspective of the institution, faculty, and students are considered. They include loss of flexibility, inconvenience, privacy concerns, security concerns, third-party involvement, extra technological requirements, extra costs, and extra effort. Effectiveness is measured as the extent to which user authentication can be confirmed. A summary of the assessment of prevention approaches and enforcement approaches are provided in the appendices (see below).

For prevention approaches, such as honor code, authentication statement, and course re-design, the extra effort put in is worthy of the benefits gained if a culture of academic integrity is developed at the institution, faculty, and student levels. However, culture is difficult if not impossible to measure objectively. As such, prevention approaches alone may not be able to

satisfy the stipulation of the Higher Education Opportunity Act as the honor code or authentication statement are not solid evidence of user authentication.

For enforcement approaches, knowledge-based and biometric authentication solutions require minimal effort and extra technologies to confirm user identity and authentication at log in. However, they are not able to prevent impersonation and collusion. In order to provide a satisfactory assurance that the registered user is the one completing the coursework, a more expensive presence authentication solution will need to be adopted.

Emerging online integrity solutions

As biometric technologies become more accurate and less costly, an authentication solution based on a unique aspect of who the user is and/or what the user does surely will replace the simplistic username and password scheme as a stronger proof of user identity, authenticity, and presence. Among the different biometric-based authentication solutions, fingerprinting is the most mature and proven technology for such purpose (Yang et al., 2011; Ratha et al., 2001). Indeed, fingerprint biometrics has already been incorporated in Apple's iPhone 5 for user identification and authentication. It is only a matter of time before a computer's input device will have a built-in fingerprint reader. As learners use such devices to interact with the virtual learning environment, their fingerprint biometrics can be examined in a continuous fashion to perform presence authentication in a non-intrusive manner.

A unimodal biometric-based authentication solution is not without its vulnerabilities and limitations. Collusion cannot be prevented if a biometrically authenticated user has someone's help in taking an exam. In addition, fingerprint biometrics will not be administrable for a student lacking this feature because of physical impairment. A multi-modal scheme for user authentication that involves surveillance technologies is therefore necessary. A bimodal scheme such as video monitoring can be used in conjunction with biometric authentication to prevent collusion. Such a scheme is less intrusive and more effective than having to re-authenticate the user when suspicious behavior is detected. A tri-modal scheme such as browser tracking and/or lock-down can also be added to video monitoring and biometric authentication to further assure that the student does not have access to unauthorized resources while taking a test. Biometric authentication adaptations or special accommodations can be made for students with disabilities. In any case, further advancement in biometric and surveillance technologies will provide institutions with more cost-effective options for online learning integrity assurance.

Predicative analytics is another area of technological advancement that holds promise in the development of next generation online integrity solutions. As students interact with the virtual learning environment, a wide variety of data such as their physical location, devices used, access patterns, learning progress, performance, etc. can be collected. These data can be mined for integrity promotion purposes. For example, student-course interaction data can produce useful information about a student's level of engagement with the course, and generate low performance and/or procrastination warnings to steer at-risk students onto a path of success. These data can also be mined for integrity enforcement purposes. Unusual or suspicious activities (e.g., students who did not do their coursework and yet have a perfect score on an exam) can be identified from the data collected so that attention can be dedicated to investigate situations of significant integrity concerns. Predictive analytics, with its ability to extract

information from data to predict trends and patterns of behavior, will be well suited in this regard.

Conclusion

We conducted a review of current approaches to online learning integrity. Existing approaches are assessed in accordance with the Higher Education Opportunity Act. Emerging technological solutions based on biometrics, surveillance, and predictive analytics are discussed. Although our review is far from exhaustive, it does provide a comprehensive overview of the cost effectiveness of different online learning integrity solutions. Institutions seeking conformance to the Higher Education Opportunity Act are urged to put in place a user authentication solution that can verify a learner's identity, authenticity, and presence. With the rapid pace of technological advancement, educational institutions will be able to implement cost-effective academic integrity solutions that are powered by sophisticated but affordable authentication hardware and software. An integrity solution that incorporates both prevention and enforcement approaches to adequately address the issues of academic integrity beyond user authentication will become a reality in the foreseeable future.

Acknowledgement

This study was presented in the 8th Annual Emerging Technologies for Online Learning International Symposium, April 22-24, 2015, with the support of the eLearning Innovation Initiative Grant at the University of Kentucky.

References

Allen, I.E., & Seaman, J. (2015). Grade Level: Tracking Online Education in the United States. Babson Survey Research Group and Quahog Research Group, LLC. Retrieved from: http://www.onlinelearningsurvey.com/reports/gradelevel.pdf

Apampa, K.M., Wills, G., & Argles, D. (2010). User Security Issues in Summative E-Assessment Security. *International Journal of Digital Society*, 1(2), 135-147.

Bailie, J.L., & Jortberg, M.A. (2009). Online Learner Authentication: Verifying the Identity of Online Users. *Journal of Online Learning and Teaching*, 5(2), 197-207.

Baron, J., & Crooks, S.M. (2005). Academic Integrity in Web Based Distance Education. *TechTrends*, 49(2), 40-45.

Bedford, W., Gregg, J., & Clinton, S. (2009). Implementing Technology to Prevent Online Cheating: A Case Study at a Small Southern Regional University. *Journal of Online Learning and Teaching*, 5(2), 230-238.

Bedford, W., Gregg, J., & Clinton. S. (2011). Preventing Online Cheating with Technology: A Pilot Study of Remote Proctor and an Update on Its Use. *Journal of Higher Education Theory and Practice*, 11(2), 41-58.

Caldwell, C. (2009). A Ten-Step Model for Academic Integrity: A Positive Approach for Business Schools. *Journal of Business Ethics*, 92(1), 1-13.

Chickering, A.W., & Reisser, I. (1993). *Education and Identity*, 2nd Edition. San Francisco: Jossey-Bass.

Chiesl, N. (2007). Pragmatic Methods to Reduce Dishonesty in Web-Based Courses. *The Quarterly Review of Distance Education*, 8(3), 203-211.

Dunn, T.P., Meine, M.F., & McCarley, J. (2010). The Remote Proctor: An Innovative Technological Solution for Online Course Integrity. *The International Journal of Technology, Knowledge and Society*, 6(1), 1-7.

Farcasin, M., & Chan-tin, E. (2015). Why We Hate IT: Two Surveys on Pre-generated and Expiring Passwords in an Academic Setting. *Security and Communication Networks*, 8, 2361-2372.

Fishman, T. (2012). The Fundamental Values of Academic Integrity. The International Center for Academic Integrity. Retrieved from: http://www.academicintegrity.org/icai/assets/Revised_FV_2014.pdf

Hart, L., & Morgan, L. (2009). Strategies for Online Test Security. *Nurse Educator*, 34(6), 249-253.

Heckler, N.C., Rice, M., and Bryan, C.H. (2013). TurnItIn Systems: A Deterrent to Plagiarism in College Classrooms. *Journal of Research on Technology in Education*, 45(3), 229-248.

Kirkpatrick, K. (2015). Technology Brings Online Education in Line with Campus Programs. *The Communications of the ACM*, 58(12), 17-19.

Kitahara, R.T., & Westfall, F. (2007). Promoting Academic Integrity in Online Distance Learning Courses. *Journal of Online Learning and Teaching*, 3(3), 265-276.

Kolberg, L. (1984). *Essays in Moral Development: The Psychology of Moral Development*, Vol. 2, New York: New York.

Inglesant, P.G., & Sasse, M.A. (2010). The True Cost of Unusable Password Policies: Password Use in the Wild. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 383-392.

Jones, I.M. (2009). Cyber-Plagiarism: Different Method Same Song. *Journal of Legal, Ethical and Regulatory Issues*, 12(1), 89-100.

Just, M., & Aspinall, D. (2009). Personal Choice and Challenge Questions: A Security and

Usability Assessment. *Proceedings of the Fifth Symposium on Usable Privacy and Security*, July 15-17.

Larson, D.K., & Sung, C. (2009). Comparing Student Performance: Online Versus Blended Versus Face-To-Face. *Journal of Asynchronous Learning Networks*, 12(1), 31-42.

LoSchiavo F.M., and Shatz, M.A. (2011). The Impact of an Honor Code on Cheating in Online Courses. *Journal of Online Learning and Teaching*, 7(2), 179-184.

Mastin, D.F., Peszka, J., & Lilly, D.R. (2009). Online Academic Integrity. *Teaching of Psychology*, 36, 174-178.

Mcallister, C., & Watkins, P. (2012). Increasing Academic Integrity in Online Classes by Fostering the Development of Self-Regulated Learning Skills. *The Clearing House*, 85, 96-101.

McNabb, L. (2010). An Update on Student Authentication: Implementation in Context. *Continuing Higher Education Review*, 74, 43-52.

McNabb, L. & Olmstead, A. (2009). Communities of Integrity in Online Courses: Faculty Member Beliefs and Strategies. *Journal of Online Learning and Teaching*, 5(2), 208-221.

Moini, A., & Madni, A.M. (2009). Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective. *IEEE Systems Journal*, 3(4), 469-476.

Moten, J., Fitterer, A., & Brazier, E. (2013). Examining Online College Cyber Cheating Methods and Prevention Measures. *Electronic Journal of e-Learning*, 11(2), 139-146.

Rabuzin, K., Baca, M., & Sajko, M. (2006). E-Learning: Biometrics as a Security Factor. *International Multi-Conference on Computing in the Global Information Technology*. 64-69.

Ratha, N.K., Connell, J.H., & Bolle, R.M. (2001). Enhancing Security and Privacy in Biometrics-based Authentication Systems. *IBM Systems Journal*, 40(3), 614-634.

Rodchua, S., Yiadom-Boakye, G., & Woolsey, R. (2011). Student Verification System for Online Assessments: Bolstering Quality and Integrity of Distance Learning. *Journal of Industrial Technology*, 27(3), 2-8.

Rowe, N.C. (2004). Cheating in Online Student Assessment: Beyond Plagiarism. *Online Journal of Distance Learning Administration*, 7(2). Retrieved from: http://www.westga.edu/~distance/ojdla/summer72/rowe72.html

Saad, L., Busteed, B., & Ogisi, M. (2013). In U.S., Online Education Rated Best for Vale and

Options. A Gallup Poll Survey. Retrieved from:: http://www.gallup.com/poll/165425/online-education-rated-best-value-options.aspx

Sewell, J.P., Frith, K.H., & Colvin, M.M. (2010). Online Assessment Strategies: A Primer. *Journal of Online Learning and Teaching*, 6(1), 297-305.

Shapley, P. (2000). On-line Education to Develop Complex Reasoning Skills in Organic Chemistry. *Journal of Asynchronous Learning Networks*, 4(2), 43-52.

Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N., & Cranor, L.F. (2010). Encountering Stronger Password Requirements: User Attitudes and Behaviors. *Proceedings of the Sixth Symposium on Usable Privacy and Security*. July 14-16.

The Higher Education Opportunity Act (2008). Retrieved from: http://www.gpo.gov/fdsys/pkg/PLAW-110publ315/pdf/PLAW-110publ315.pdf

Ullah, A., Xiao, H., Lilley, M., & Barker, T. (2012). Using Challenging Questions for Student Authentication in Online Examination. *International Journal for Infonomics*, 5(3/4), 631-639.

Vandehey, M., Diekhoff, G., & LaBeff, E. (2007). College Cheating: A Twenty-Year Follow-Up and the Addition of an Honor Code. *Journal of College Student Development*, 48(4), 468-480.

Yang, J., Xiong, N., Vasilakos, A.V., Fang, Z., Park, D., Xu, X., Yoon, S., Xie, S., & Yang, Y. (2011). A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing. Communications," *IEEE Systems Journal*, 5(4), 574-583.

Appendices

Table 1. The Cost Effectiveness of Prevention Approaches to Online Learning Integrity

Integrity solution	Student costs	Faculty costs	Institution costs	Effectiveness
Honor code	Annoyed with frequent reminder of the code. (Vandehey et al., 2007)	Extra work in reminding students about the code. (Chiesl, 2007)	Extra work in enforcing the code consistently. (Caldwell, 2009; Baron and Crooks, 2005)	A weak evidence of students' commitment to honor the code. No preventing of impersonation. (LoSchiavo & Shatz, 2011; Hart & Morgan, 2009; Kitahara and Westfall, 2007)
Authenticity statement	Annoyed with frequent signing of statements. (Vandehey et al., 2007)	Extra work in preparing and collecting the statement. (Caldwell, 2009)	Extra work in enforcing the statement consistently. (Caldwell, 2009)	A weak evidence of students' honesty. No preventing of impersonation. (Hart & Morgan, 2009; Mastin et al., 2009)
Course re-design	None (Caldwell, 2009; Chiesl, 2007)	Extra work in re-designing and delivering the course. (Hart & Morgan, 2009; McNabb and Olmstead, 2009)	Extra work in enforcing the solution consistently. (Caldwell, 2009)	A weak assurance of integrity. No preventing of impersonation. (Hart & Morgan, 2009; Rowe, 2004)
User id and password	Annoyed with frequent updates of a strong password. (Farcasin and Chan-tin, 2015)	None (Shay et al., 2010; Inglesant and Sasse, 2010)	Extra work to securely store, match, and update a user's id and password. (Shay et al., 2010; Inglesant and Sasse, 2010)	A strong evidence of user identity confirmation. No preventing of impersonation. (Ullah et al., 2012; Bailie & Jortberg, 2009)
Challenging or security questions	Annoyed with frequent questionings. (Hart & Morgan, 2009; Just & Aspinall 2009)	None (Just & Aspinall 2009)	Extra work to securely store, match and update a user's challenging questions. (Baili & Jortberg, 2009)	A strong evidence of user identity confirmation. No preventing of impersonation. (Ullah et al., 2012; Bailie & Jortberg, 2009)

Table 2. The Cost Effectiveness of Enforcement Approaches to Online Learning Integrity

Integrity solution	Student costs	Faculty costs	Institution costs	Effectiveness
Biometrics	Extra device to read biometrics. Privacy concerns. (Ullah et al., 2012; Rodchua et al., 2011; Bailie & Jortberg, 2009)	None (Bedford et al., 2011)	Extra work to securely store and match a user's biometrics. (Bailie & Jortberg, 2009)	A strong evidence of user identity and authenticity confirmation. No preventing of impersonation after login. (Bedford et al., 2011; Dunn et al., 2010)
Biometrics re-authentication	Extra device to read biometrics. Privacy concerns. Annoyed with frequent re-authentications. (Apamap et al., 2010)	None (Bedford et al., 2011)	Extra work to securely store and match a user's biometrics. Extra work to process a random re-authentication. (Moini and Madni, 2009)	Prevention of impersonation. No prevention of collusion. (Apampa et al., 2010; Moini & Madni, 2009)
Video monitoring	Extra device to record video. Privacy concerns. (Rodchua et al., 2011; Bedford et al., 2009; Hart & Morgan, 2009)	Extra work to analyze video footage. (Apampa et al., 2010; Bedford et al., 2009)	Extra work and costs to securely store and retrieve a user's video footage. (Bedford et al., 2011)	Prevention of impersonation. Prevention of collusion. (Bedford et al., 2011)
Face-to-face proctoring	Extra effort to be physically present at an agreed time and place. Extra cost for taking proctored exams. (McNabb, 2010; Bailie & Jortberg, 2009; Hart & Morgan, 2009)	Extra work to arrange for proctoring. (Bailie & Jortberg, 2009)	Extra work and cost to provide a testing center or endorse a trustworthy third party provider. (Bailie & Jortberg, 2009)	Prevention of impersonation and collusion only if the proctor is trustworthy. (Kirkpatrick, 2015)
Virtual proctoring	Extra cost for taking proctored exams. Extra cost for proctoring equipment. Privacy concerns. (Kirkpatrick, 2015; Rodchua et al., 2011)	Extra work to arrange for proctoring. (Kirkpatrick, 2015)	Extra work and cost to provide a proctoring center or endorse a trustworthy third party provider. (Kirkpatrick, 2015)	Prevention of impersonation and collusion only if the provider is trustworthy. (Kirkpatrick, 2015; Bedford et al., 2011)