

Can We Prevent a Technological Arms Race in University Student Cheating?

Joseph Mortati and Erran Carmel, American University

This column surveys the technologies and techniques that both sides—students and instructors—use in the arms race. We discuss the risks, the false positives, and threats to privacy.

The pandemic elevated *academic integrity* issues (also known as cheating) related to the authorship of digitally submitted assignments. In this context, authorship answers the question did the student actually complete any of the assignment/exam? There is now a large gray market out there in cheating services: companies offering options that range from databases of papers, to completing custom assignments, and up to and including attending online classes for students (with a guarantee of an A or B). To ensure

academic integrity in an online educational world, what's needed are innovative ways of ensuring authorship of digital work. Clearly, a technological arms race is bad for students and faculty—and for society at large. This column will survey the technologies that both sides use. We then touch on governance approaches, false positives, and threats to privacy.

THE PROBLEM OF AUTHORSHIP IDENTITY IN EDUCATION

The authorship of digital academic assignments, whether exams, papers, or computer code, cannot be necessarily assured. While this was true before the pandemic, the issue was exacerbated with large-scale migration to the relative anonymity of online classes. The challenge is can we be vigilant in a new, online world while maintaining students' best interests at heart?

Prepandemic studies in the United States showed as much as 50% of college students cheated at some point.²¹ While large-scale studies are not yet available, there is strong evidence from multiple universities in the United



States and the United Kingdom that saw increases in both exam content being available online (for example, on chegg.com) and/or prosecutions for academic integrity.⁹

A BATTLE OF TECHNOLOGIES

What technologies do students have? We begin with a low-end clever trick. The student uploads an assignment through a third-party website that deliberately corrupts the document, preventing it from opening.⁶ The instructor then politely notifies the student to resubmit the file. This could be days or weeks depending on instructor grading load, which gives the student more time to complete the assignment.

Pandemic-induced online exams were often made available over a period of several days. While this provided flexibility for students, it allowed some of them to share exam data on multiple digital channels. Websites like Chegg and CourseHero (www.coursehero.com) allow students to upload the exam and its answers.

A particularly pernicious weapon is known as *contract cheating*: hiring someone to complete an assignment for you,⁷ euphemistically known as the “academic writing business.” This is done through electronic marketplaces where freelancers offer work for hire. Contract cheating expands dishonesty beyond doing simple look up the answers for you by completing higher-level thinking assignments and also creative writing endeavors. A study in the United Kingdom showed that, between 2014 and 2018, 15.7% of students self-reported some form of contract cheating.¹⁵ Such cheating can even include taking an online course for the student with a guaranteed grade outcome. As *Chronicle of Higher Education* put it in the October 2020 article “Students Cheat. How Much Does It Matter?,” paying a third party to do a

student’s work is “not cutting corners, it’s paying someone else to run the race.”²⁰ Unfortunately, it is both the most effective form of cheating and the most difficult to detect.

WHAT TECHNOLOGIES DO INSTRUCTORS HAVE?

First, multiple technologies are needed for exams. Lockdown browsers (for

browser: bandwidth limits, the need for a webcam, privacy concerns, and repressive governments blocking access to educational websites.

One avenue to check on suspicious activities is tracking a student’s Internet Protocol (IP) address location, though students can trick this with virtual private networks (VPNs) and other resources. Universities can use IP range

The challenge is can we be vigilant in a new, online world while maintaining students’ best interests at heart?

example, Respondus) prevent the student from accessing any other webpages or applications on that device during an exam. However, the student who is intent on cheating can easily rely on other devices or close-by humans. An escalated technology is called *proctored testing* (for example, Proctorio’s Online Proctoring), which uses identification verification and automated monitoring (with or without live monitoring via webcam).²⁵ Many instructors used casual video monitoring during the pandemic by requiring students to have Zoom video on during the exam. Thus, the findings from a study by Alessio et al. are enlightening. This 2017 U.S.-based study showed that digital exam proctoring lowered student scores significantly. Specifically, tests with live video monitoring (that is, humans who reviewed the recordings after the exams, which were closed-book/notes, and notified instructors of possible violations) resulted in scores 17 points lower than students enrolled in the same courses without test proctoring. This suggests that unproctored tests may lead to more cheating.¹ However, there are limitations to video monitoring—with or without a lockdown

blocking to force students to either be on campus or use a particular VPN, but this may prevent a user from accessing a learning management system (LMS). However, given that postpandemic students are literally scattered globally, what can the IP address really assure us about a student’s integrity?

Anti plagiarism software (for example, TurnItIn and SafeAssign) is a more-nuanced technology. However, such applications can only detect the level of originality as an indicator of plagiarism. This means they are not “plagiarism detectors” but tools to guide faculty in assessing the student’s work. While they can be a deterrent to improper copy and paste or failure to cite sources, they cannot determine who *authored* the file. Nevertheless, there is some positive news. A 2020 study from 12 semesters of academic misconduct data ($n = 12,937$) at a Vietnamese university showed a 37% reduction in instances of suspected plagiarism using Turnitin.¹⁶

NEW TOOLS TO DETER OR DETECT CHEATING

Distance introduces a challenge that was once rather unusual: ascertaining strong identity binding. In the United

States, the Higher Education Opportunity Act of 2008 requires institutions, at their option, to “verify identities of remote students by using a secure login and pass code, proctored examinations, or new or other technologies and practices that are effective verifying student identification.”²⁴ The Vietnamese study mentioned earlier could not rule out contract cheating.

Identity verification can use multifactor authentication, which is what banks usually use for remote access. A step up is biometrics. Primary biometric authentication verifies identity based on physical things like fingerprints or facial patterns. This is better suited to verifying students attending a synchronous class (to deter someone else taking the class for them) or a video-proctored exam (to ensure the test-taker is who they say they are).

Secondary biometric authentication verifies identity based on behavioral patterns—and may be a future tool in the cheating arms race. One form

network, decision tree, and support vector machines) showed an accuracy rate using a two-sentence sample of 53–99%. While keystroke dynamics are intended to supplant or augment usernames and passwords, they could be adapted to an academic setting and extended to help identify a test-taker.

In 2019, TurnItIn launched a new application called “Authorship Investigate.” It uses an algorithmic combination of a readability scale (to judge the complexity of the text), metadata analysis, punctuation use, and a vocabulary check to compare differences in written work.²³ While this is a potentially important step forward, it is not yet clear what the accuracy rate is or at least what percentage are false positives. Likewise, this software uses an algorithm that analyzes a student’s writing over time and compares it to the “norm”. But what if the starting point norm is not the student’s own work? What if the student uses the same third-party “supplier” for all their coursework?

Such cheating can even include taking an online course for the student with a guaranteed grade outcome.

of this captures keystroke dynamics by monitoring a user’s typing style looking for patterns. That is, “[It’s] not what you type, but *how* you type.”¹⁴ This is similar to clickstream analytics, commonly used in e-commerce, to identify user “signature” patterns of navigating within a website.² A newer approach to this, tested in 2019,³ used a combination of three time-related variables (measured in microseconds): held time (the time between when a key is pressed and released), up-down time (the time between the first key being released and the second being pressed) and down-down time (the sum of these two times). Preliminary results, using four machine learning algorithms (random forest, neural

RISKS WITH TECHNOLOGY

One of the risks with any software-based approach is false positives. Here are two recent examples. In October 2020, the California (law school) bar exam was administered using ExamSoft, which prevents users from having other applications open, along with video monitoring. Approximately 3,200 test-takers were flagged for cheating (nearly one-third of the total), including some who took the test at major law firms where human proctors were also present.¹¹ Technical anomalies flagged some test-takers as suspicious (for example, some people using Lenovo laptops, which prevented ExamSoft access to the internal microphone).¹² A follow-up investigation by the California State Bar Association

could only affirm 47 cases (about 1.5%) were “indisputable” offenses.¹⁰

Another example of misused surveillance technology, reported by *The New York Times*,¹⁸ took place at Dartmouth Medical School, which charged 17 students with cheating by using technology as evidence. The students took an online exam using ExamSoft without video monitoring, but the separate Canvas LMS showed the students were logged into other resources at the same time. At issue was whether such accesses were intentional or due to Canvas automatically generating activity data (for example, the student could have remained logged into Canvas on a mobile device while taking the exam). After much backlash, all honor code charges against these students were dropped.¹⁹

PRIVACY CONCERNS

Not only do the tools have false positives, but also all of these antichecking technologies harbor within them *incursions into student privacy*. Should an LMS be used as a surveillance tool? For years, instructors had the ability to peek into students’ lives to see when Johnny logged on (was it at 3 a.m.?). Any kind of monitoring and tracking is a privacy threat. Boundaries are often arbitrary, in the eye of the beholder. One person may see remote exam monitoring as “invasive” or “Orwellian” but view the same human and electronic surveillance inside a traditional classroom as acceptable. Academia has a difficult tradeoff to navigate: the arms race has changed the game by providing students with a new cheating arsenal (and more customers for contract cheating entities). This means that academic integrity technologies will have to be able to appropriately monitor student activities without violations of privacy and ensuring due process is provided.

ACADEMIC INTEGRITY AS AN INFORMATION SECURITY ISSUE

While all universities have academic integrity policies, current norms

require that faculty, with limited support and guidance from administration, be the focal point for deterring and detecting academic dishonesty. We argue the issue of authorship identity—as to assessing grades and awarding academic credit—is so important that it should be elevated to a higher level of scrutiny as an *information security issue*. By U.S. law, universities are required to secure student information under the Family Educational Rights and Privacy Act and the Health Insurance Portability and Accountability Act. Why, then, is something as important as conferring degrees not a matter of information security as well? For example, in 2020, *Los Angeles Times* reported that a very wealthy University of Southern California stu-

people involved in carrying out or monitoring assignments—students, faculty, teaching assistants, and staff—need education in ethical academic conduct. For starters, as a way of reducing cheating, create an environment that values competence and mastery over grades. That is, help students understand the benefits of “why” this assignment is important to them and the consequences of cheating.

Processes

Courses can be better designed to be more engaging, include clearer and more helpful policies. In addition, courses should use strategies to mitigate cheating (for example, more open-ended questions and assignments that change regularly). Likewise, make learning less

of ensuring authorship of a given file. Absent this, a range of strategies from reducing cheating attempts before they start (the best method) to a defense-in-depth approach is the best way forward to reduce the effects of an educational arms race. ■

REFERENCES

1. H. M. Alessio, N. Malay, K. Maurer, A. J. Bailer, and B. Rubin, “Examining the effect of proctoring on online test scores,” *Online Learn.*, vol. 21, no. 1, pp. 146–161, 2017. [Online]. Available: <https://files.eric.ed.gov/fulltext/EJ1140251.pdf>. doi: 10.24059/olj.v21i1.885.
2. D. Amo Filvà, M. Alier Forment, F. J. García-Peñalvo, D. Fonseca Escudero, and M. J. Casañ, “Clickstream for learning analytics to assess students’ behavior with Scratch,” *Future Gener. Comput. Syst.*, vol. 93, pp. 673–686, Apr. 2019. [Online]. Available: <https://upcommons.upc.edu/bitstream/handle/2117/130122/Clickstream%20for%20learning%20analytics%20to%20assess%20students%20behavior%20in%20scratch.pdf;sequence=6>. doi: 10.1016/j.future.2018.10.057.
3. T. Attaie, J. Caldwell, T. Ward, Y. Yassin, J. Graham, and K. Elliot, “Dynamic keystroke for authentication with machine learning algorithms,” in *Proc. IEEE SEC DEV*, McLean Virginia, Oct. 2019, pp. 19–20. [Online]. Available: https://www.researchgate.net/publication/336683999_Dynamic_Keystroke_for_Authentication_with_Machine_Learning_Algorithms
4. L. Z. Bain, “How students use technology to cheat and what faculty can do about it,” *Inform. Syst. Educ. J.*, vol. 13, no. 5, pp. 92–99, 2015.
5. D. Brown, “Students are still using tech to cheat on exams, but things are getting more advanced,” *USA Today*, Aug. 21, 2019. <https://www.usatoday.com/story/tech/2019/08/16/how-teachers-preventing-high-tech-cheating-classroom/2017389001/>

Primary biometric authentication verifies identity based on physical things like fingerprints or facial patterns.

dent, who rarely attended class and had others do his schoolwork, earned both a bachelor’s and a master’s degree.¹⁷ While this case is extreme, the identity and authorship implications for online classes are staggering. How can accredited schools claim the validity of conferred degrees in the new environment?

A WAY FORWARD

The pandemic has exposed universities as ill-prepared to deal with the mass adoption of online classes and a new generation of cheating. It’s not a popular topic for provosts and deans to spend time on because it’s so difficult. However, taking a people–processes–technology approach identifies the important and complementary factors that can be used going forward.

People

The people involved need to understand the issues. This means all

about rote recall, have some assignments that are personalized, be more engaged with your students, and have multiple and varied assessments versus just a few large exams or papers. This will reduce the incentive to cheat.

Technology

In this fast-changing landscape, forcing a choice among myriad technology solutions should not be left to individual instructors to figure out because their primary responsibility is student learning and well-being. Likewise, the cat-and-mouse game is moving more quickly than many instructors can keep up with. Instead, consider making academic integrity a part of information security policies, as is done with other student records.

In conclusion, as with most difficult problems, there is no silver bullet. But if there was one, it would be an accurate, reliable, noninvasive way

6. S. LaConte, "A TikTok found a clever (But Bad!) hack to help students cheat on their homework and it's going viral," *Buzzfeed*, May 19, 2020. <https://www.buzzfeed.com/stephenlaconte/viral-tiktok-how-to-cheat-home-work-assignments-corrupt-my>
7. R. Clarke and T. Lancaster, "Establishing a systematic six-stage process for detecting contract cheating," in *Proc. 2nd Int. Conf. Pervasive Comput. Appl.*, New York, 2007, pp. 342–247. [Online]. Available: <https://ieeexplore.ieee.org/document/4365466>. doi: 10.1109/ICPCA.2007.4365466.
8. R. Clarke, and T. Lancaster, "Commercial aspects of contract cheating," in *Proc. 18th ACM Conf. Innovation Technol. Comput. Sci. Educ.*, New York, 2013, pp. 219–224. [Online]. Available: <https://dl.acm.org/doi/10.1145/2462476.2462497>. doi: 10.1145/2462476.2462497.
9. S. Subin, "How college students learned new ways to cheat during pandemic remote schooling," *CNBC*, Mar 21, 2021. <https://www.cnbc.com/2021/03/21/how-college-students-learned-new-ways-to-cheat-during-covid-.html>
10. J. E. Cutler and S. Skolnik, "California bar exam pass rate spikes in first-ever online test," *Bloomberg Law*, Jan. 8, 2021. <https://news.bloomberglaw.com/social-justice/california-bar-exam-pass-rate-spikes-in-first-ever-online-test?context=article-related>
11. "Flagging isn't the same as cheating," *ExamSoft*. <https://examsoft.com/resources/flagging-isnt-cheating> (accessed May 26, 2021).
12. J. Kelley, "ExamSoft flags one-third of California bar exam test takers for cheating," *Electronic Frontier Foundation*, Dec. 22, 2020. <https://www.eff.org/deeplinks/2020/12/examsoft-flags-one-third-california-bar-exam-test-takers-cheating>
13. D. Lederman, "Best way to stop cheating in online courses? 'Teach Better,'" *Inside Higher Ed*, July 22, 2020. <https://www.insidehighered.com/digital-learning/article/2020/07/22/technology-best-way-stop-online-cheating-no-experts-say-better>
14. F. Monroe and A. D. Rubin, "Key-stroke dynamics as a biometric for authentication," *Future Gener. Comput. Syst.*, vol. 16, no. 4, pp. 351–359, 2000. [Online]. Available: <https://www.cs.columbia.edu/~hgs/teaching/security/hw/keystroke.pdf>. doi: 10.1016/S0167-739X(99)00059-X.
15. P. M. Newton, "How common is commercial contract cheating in higher education and is it increasing? A systematic review," *Front. Educ.*, vol. 3, p. 67, Aug. 30, 2018. doi: 10.3389/feduc.2018.00067.
16. M. Perkins, U. Basar Gezgin, and J. Roe, "Reducing plagiarism through academic misconduct education," *Int. J. Educ. Integrity*, vol. 16, no. 1, pp. 1–15, 2020. doi: 10.1007/s40979-020-00052-8.
17. H. Ryan and M. Hamilton, "The true story of the heartthrob prince of Qatar and his time at USC," *Los Angeles Times*, July 16, 2020. <https://www.latimes.com/california/story/2020-07-16/qatar-prince-usc-ucla-la>
18. N. Singer and A. Krolik, "Online Cheating charges upend Dartmouth Medical School," *NY Times*, May 9, 2021. <https://www.nytimes.com/2021/05/09/technology/dartmouth-geisel-medical-cheating.html>
19. N. Singer, "Dartmouth Medical School drops online cheating cases against students," *NY Times*, June 10, 2021. <https://www.nytimes.com/2021/06/10/technology/dartmouth-cheating-charges.html>
20. B. Supiano, "Students cheat how much does it matter?" *The Chronicle of Higher Education*, Oct. 21, 2020. <https://www.chronicle.com/article/students-cheat-how-much-does-it-matter>
21. "The reality of cheating in college," *Best Value Schools*, Mar. 4, 2021. <https://www.bestvalueschools.org/reality-cheating-college/>
22. K. Trezise, T. Ryan, P. de Barba, and G. Kennedy, "Detecting academic misconduct using learning analytics," *J. Learn. Analytics*, vol. 6, no. 3, pp. 90–104, 2019. doi: 10.18608/jla.2019.63.11.
23. "Turnitin authorship investigate supporting academic integrity is released to higher education market," *Turnitin*, Mar. 13, 2019. <https://www.turnitin.com/press/authorship-released-to-higher-education-market>
24. "Higher education opportunity Act," U.S. Department of Education, 2008. <https://www2.ed.gov/policy/highered/reg/hearulemaking/2009/accred-regsnegotiated.pdf>
25. A. Wolfe, "How to identify and prevent contract cheating," *Journal of Accountancy*, Feb. 12, 2019. <https://www.journalofaccountancy.com/newsletters/extra-credit/contract-cheating.html>

JOSEPH MORTATI is a senior professorial lecturer at the Kogod School of Business at American University, Washington, D.C., 20016, USA. Contact him at mortati@american.edu.

ERRAN CARMEL is a professor of information technology at the Kogod School, Washington, D.C., 20016, USA. Contact him at carmel@american.edu.