

Chapter 9

Ethics, EdTech, and the Rise of Contract Cheating



Brenna Clarke Gray 

Abstract This chapter argues that establishing a “culture of academic integrity,” in the era of digitally-situated plagiarism like contract cheating, begins with an institutional approach to student data and student work that is rooted in ethics. If “students cheat when they feel cheated” (Christensen Hughes, 2017, p. 57), then the ethical failures inherent in a system-wide move toward for-profit homework systems and plagiarism checkers sets a dangerous model for students to follow. We are responsible for modelling for our students what it looks like to be a contributing member of an academic community, and we do so by taking seriously our students, their data, and their work, and not only when it comes time to run it through a plagiarism detector or check their IDs against a proctoring software. This chapter argues that a more responsible relationship to student data, and a less cozy relationship with for-profit educational technologies, is required if our institutions are serious about fostering a culture of academic integrity.

Keywords Academic integrity · Algorithm · Data · Canada · Contract cheating · Privacy

Introduction

When we introduce to our students the idea of establishing a “culture of academic integrity,” we typically frame the discussion primarily around the responsibilities of students. In my own syllabi as an instructor, I talk about academic integrity embodying everything from explicit skills like correctly citing sources, to more intangible concepts like coming to class prepared and treating colleagues with respect.

The original version of this chapter was revised: The incorrect lines in the Abstract has been removed. The correction to this chapter can be found at https://doi.org/10.1007/978-3-030-83255-1_33

B. C. Gray (✉)
Thompson Rivers University, Kamloops, Canada
e-mail: bgray@tru.ca

© The Author(s) 2022, corrected publication 2022
S. E. Eaton and J. Christensen Hughes (eds.), *Academic Integrity in Canada*,
Ethics and Integrity in Educational Contexts 1,
https://doi.org/10.1007/978-3-030-83255-1_9

Faculty know that they, too—whether through scholarly associations, granting agencies, or their own internal ethical compass—have a commitment to academic integrity. But when we frame academic integrity for students, that component is rarely discussed. It's common in higher education circles to hear about the notion of creating a culture of academic integrity (Hendershott et al, 2000), but definitions of what such an academic culture would look like vary widely (Macfarlane et. al., 2014). While most institutions focus on student responsibilities vis-à-vis academic integrity, it is rarer to see the conversation extend to the responsibilities of faculty, though the power of faculty modeling—such as with citations in slide decks and careful attention to reuse of content like images—is significant in helping students to understand the norms of their discipline regarding academic integrity (Robinson & Glanzer, 2017). Institutional policies and campus training programs focus on students. But modelling a culture of academic integrity begins with what happens in the classroom and across the institution, and as violations of academic integrity go high-tech with the rise of contract cheating, institutions must reckon with the way their data privacy and educational technology policies and practices fail to model academic integrity. In this chapter, I argue that the contract cheating epidemic can be insulated against with a renewed attention to ethical pedagogical strategies in the deployment of educational technologies. Given the explosive growth of the contract cheating problem and the huge money it makes for unethical players, it is imperative that post-secondary institutions protect students by all possible means, including examining their own cultures of academic integrity in the digital space. Canadian higher education—and indeed, higher education globally—has not to this point had a sector-wide conversation about ethics in educational technologies, and our institutions as a result often engage in practices and contracts with private, for-profit companies that include data agreements that would never pass an equivalent of a Research Ethics Board (Stewart, 2020).

This chapter focuses specifically on the failure of academic integrity known as contract cheating. This is cheating that takes the form of students hiring third parties—sometimes across the globe—to submit one or all of their assignments in a class for them. Contract cheating is not a situation of individual students in a course making poor choices: it's a business. There has always been opportunity for students with financial means to purchase coursework from colleagues, but now the gig economy and the easy ability to transfer data means that people—perhaps as far away as Kenya (Lancaster, 2019a)—are earning comparatively small amounts of money to produce intellectual labour which is then sold to desperate students in North America and Europe, particularly in English-speaking countries, for big profit (Rigby, 2014). It's hard to track by traditional means either pedagogical or technological; if every assignment in a course is created by someone else, the instructor has no grounds for comparison, and many of these companies proudly proclaim their high originality scores on Turnitin because, of course, the work is original—it just wasn't written by the student (Cadloff, 2018; Peterson, 2019). As a result, there is probably more of it happening even than we think (Eaton, 2020). And it makes a lot of money globally (Rigby, 2014; Ellis et al., 2018).

I am interested, though, in how the same practices we see engaged in by institutions and educational technology companies—a devaluing and de-prioritization of original work when it comes to the classroom space, predatory relationships between consumers and service providers, and a cavalier approach to handling data privacy—are echoed and magnified by contract cheating firms. I argue that a more responsible relationship to student data, and a less cozy relationship with for-profit educational technologies, is required if our institutions are serious about fostering a culture of academic integrity.

De-Valuing and De-Prioritizing Original Work in the Classroom

At the 2019 Academic Integrity Day held at Thompson Rivers University, student union groups repeatedly raised the issue of reciprocity and respect as critical to conversations about why students cheat. One student union representative specifically asked how students can be expected to feel a sense of responsibility over their own learning in courses increasingly taught using tools like for-profit homework systems or courseware¹ and publisher-provided lecture slides: “If you can buy your lectures and assignments,” he asked the assembled professors and administrators, “why can’t I buy my submissions?”² This echoes Julia Christensen Hughes’ observation from reviewing student explanations of academic dishonesty that “students cheat when they feel cheated” (Christensen Hughes, 2017, p. 57). Added to this are the privacy and security issues enmeshed in homework systems, which at least in part monetize student data while simultaneously charging them for the opportunity to submit their coursework in classes for which they are already paying tuition (UNESCO IITE, 2020; Senack et al., 2016). Although there are good and compelling reasons why professors opt to use these kinds of tools, including an increasingly precarious professoriate, the pressures of producing research, and the additional stresses imposed by restructuring institutions in the wake of Covid-19, institutions, the message we send to students becomes deeply complicated. What does it mean to foster a culture of academic integrity across a university, and what does it mean to act with integrity—and does the responsibility only fall on students? If we truly wish to model academic integrity, the answer to the latter question must be no: if the stakes of academic integrity truly matter, our students should see us all embodying it (Morris, 2016).

As universities integrate ever more completely with large, for-profit educational technologies companies, they burrow ever deeper into troubling agreements where

¹ Homework systems, courseware, and “course-in-a-box” are all synonyms for a class of edtech products provided primarily by textbook publishers, either as value-adds to traditional textbooks or stand-alone products. There is typically an added cost to students. Increasingly, we see courseware and homework systems as significant elements of the classroom experience for students; some of these tools are the primary means by which students submit homework, and these systems typically include exams, assignment prompts, and often even lecture materials.

² The identity of the student is kept confidential. Personal communication, 18 October 2019.

student data is monetized now or in perpetuity. In addition to troubling data practices, many of the solutions heralded as tools in the fight for academic integrity, whether plagiarism detection software or e-proctoring platforms, engage in questionable ethical practices like profiling student behaviour (Swauger, 2020). Turnitin, for example, has access to wide swaths of student data in the form of essays and assignments, which they mine in order to be able to compare submissions to their database to assess whether student work has been copied. Their business model relies on receiving student intellectual property for free—students, of course, are not compensated for providing the content for their database—and has expanded to include a Revision Assistant tool for students that is also built from this massive amount of student data (Stommel & Morris, 2017). Revision Assistant, designed to help students identify errors in their writing prior to submission, is, in essence, a machine-taught tool to improve writing based on the vast swaths of student writing Turnitin’s larger database can analyze. Are students fully informed about where their data is going, in this context, and who is profiting from it? Increasingly, we’re seeing student groups advocate for more transparency in the use of Turnitin, and for opt-out policies to be made more explicit. Much of the way Turnitin is used in Canada—far less ubiquitously than elsewhere—is due to Jesse Rosenfeld’s landmark legal action against Turnitin; Rosenfeld argued successfully that students should not be presumed guilty, which is the position from which all plagiarism detection software begins, but also that students should not be compelled to waive their copyright in order to be evaluated (Purdy, 2005). Instructors can ask to have the work their students submit deleted from the Turnitin database, but they have to know to ask. Turnitin has always downplayed the data mining they do, but it is the backbone of their ability to offer their service. It’s also what makes them attractive to venture capitalists. In March 2019, Turnitin was acquired by a venture capital firm for US\$1.75B, which gives you a sense of what all that uncompensated student intellectual property and mined data is worth (Luke, 2019).

And many of these companies impose on the central tenets at the core of university life, by holding institutions to restrictive non-disparagement clauses that limit the freedom of speech and critique of students, staff, and faculty alike, even sometimes when they are never party to the original agreement. The CEO of TopHat, for example, likes to talk about how much data they have access to, and that they can drill down into it enough to analyze individual student study habits (Zubair, 2017). But the End User License Agreement for TopHat includes provisions that students cannot link to TopHat in an article critical of its use, students are responsible for any data breeches that occur, and they offer no opt-outs for the collection of personal data beyond opting out of the service altogether (Rhineland, 2017). When educational institutions contract with these firms, they believe the gain is greater than the loss; this is the same logic that drives desperate students to the essay mill, and it’s equally misguided in both cases. If our integrity as institutions can be chipped away at through predatory agreements that disrupt the very mission of our institutions, can we be surprised when we see students engaging in the equivalent?

Predatory Relationships with For-Profit EdTech

For-profit educational technology companies—in contrast with open or publicly-funded edtech projects—can make money in a limited number of ways: they can sell an individual or an institution one-shot products, they can offer a subscription model that is institution-paid or student-paid, or they can sell the data they collect. Or some combination of the above. Many of the agreements our institutions sign with these companies give explicit rights to use student data for things like “targeted marketing,” and opt-outs are complicated and Byzantine (American Association of University Professors, n.d.). In 2012, for example, the former textbook, now primarily data, company Pearson boasted that they have more access to student data in K-12 than anyone in the world (Office of EdTech, 2012). In the higher education space, Pearson is the biggest player, and they have some incredible access to student data, including everything from financial aid applications to interim and final grades. They say they don’t sell student data, but they also publicly refused to sign the Student Privacy Pledge. And recently, the inevitable happened: a data breach, exposing data from 13,000 institutions and one million college students. The attack occurred in November of 2018, but Pearson waited to inform the FBI until the following March, and end users were not notified until August. While Pearson asserts that the breach was “limited” to first and last name, date of birth, and email address—enough to do a fair amount of damage!—it impacted data collected as early as 2001 (Olson, 2019). The roll out of the disclosure (and the disappearance of the statement from their website) suggests that the top priority in this instance wasn’t ever student data, but brand management.

When students contract with cheating companies, they usually are required to hand over a lot of personal data, some of which should be specifically of concern to universities. Students give up credit card information, yes, and, distressingly, their social insurance numbers (SIN; the primary government identification number in Canada, similar to the SSN in the US); they also give up their student ID numbers and Learning Management System login information to companies with very limited privacy protections (Sutherland-Smith & Dullaghan, 2019). Certainly, giving up a credit card number and SIN can have far-reaching impacts for the student for years to come; handing over a student ID and login information is how contract cheating firms, once established at a university, experience exponential growth. Once a contract cheating firm has private student information, students become easily exploited; contract cheating companies have been reported to continue to extract money from students well after they have completed the course for which they contracted the service in the first place, and when students stop paying the extortion, the companies report the original act of plagiarism to the university (Yorke et al, 2020). The threat of this happening can keep a student in a cycle of contracting with the company, or recommending the service to their classmates, since they believe they will be reported if they do not. Further, I know from my own observation that once a contract cheating firm has access to the Learning Management System at an institution, their access to students grows rapidly: they can access course materials, view assignments, and

directly message other students in the course in order to find new clients. They can access the data not only of the person for whom they are uploading assignments, but they can access class lists and steal the intellectual property of the class professor, too; this material will likely be reused and resold by the company. And depending on the practices of the company, it can be hard for IT Services to flag and block this activity.

Why do students feel comfortable sharing something as critical to the integrity of the university as their LMS login information in the first place? There is a lot of rhetoric about so-called digital native³ students and their supposed disinterest in data privacy, but research does not support this assumption; on the contrary, students are increasingly concerned about these issues, but a lack of information and a lack of empowerment drives poor choices (Hargiatti & Marwick, 2016). Our traditional-age students have been raised in an informational ecosystem where companies like Google and Facebook know everything about them (and increasingly, they have had a presence on these networks before they were meaningfully able to consent to it) and then they go to university and interact daily with companies like Pearson, Turnitin, and TopHat who are monetizing their data with the express consent of their institutions. Perhaps instead of questioning their lack of care about their privacy and data, we might question whether they have ever felt empowered to resist these corporations, and it's worth considering whether institutions have treated seriously enough the fiduciary responsibility they hold over data when it comes to Big Tech.

Contract Cheating as Case Study

The practices by which contract cheating companies find our students are worth exploring as one example of this kind of shadowing between the emergence of practices in higher education and their exploitation by companies whose influence we seek to reduce. Algorithms are all around us, and they drive a substantial amount of decision-making. They also are not inherently bad or damaging: in its most basic form, it is a set of instructions that determines a series of outputs from a series of inputs. And we are surrounded by algorithmic processes all the time. It's an algorithm that drives what Netflix thinks you want to watch next, what Instagram thinks you might click-through to buy, and what Google anticipates you want from your search results. These experiences are sometimes creepy—like when a store you shop at knows before you do that you are pregnant (Hill, 2012)—and often aggressively capitalist, but they aren't necessarily explicitly harmful.

Algorithms are not neutral, however. Instead, algorithms reflect the old adage of “garbage in, garbage out,” which is to say that whatever biases underwrite the

³ Mark Prensky coined this term in 2001, but it has been rightly challenged conceptually. In particular, being raised with a tool and even using it extensively for social purposes does not train one to use the tool critically or in a manner commensurate with expectations of higher education. Erika Smith's (2012) review of the literature on the concept is a useful tool.

programming of an algorithm will be reflected in its outputs (Stinson, 2020). And, since we live in a society that wrestles with racism, sexism, classism, ableism, and many other inequities, we should not be surprised that algorithms are often built in a way that encompasses many of these inequities. Virginia Eubanks described the use of algorithms in the development of social programming as an “empathy override,” a decision to outsource perceptions about who “deserves” care (Eubanks, 2018). This is a way of not having harder and more complex political conversations, and it relies on a scarcity model of resourcing social programs and care. Those are conversations that are important to have and will be shaped by individual values, but we have to have them, and not hide behind assumptions that these processes are somehow neutral.

What algorithms, for example, make decisions about who is a good bet for a mortgage or business loan, and what assumptions underlie those parameters? We see algorithms used to redraw community boundaries to further disenfranchise the poor and the marginalized. There’s a term for this: digital redlining (Gilliard, 2017). Indeed, just as old-fashioned analog redlining worked in the service of segregation and reduced class mobility, digital redlining has a direct impact on socioeconomic mobility. Algorithmic processes are increasingly used by credit bureaus to analyze your social media connections, making judgements about financial solvency in part based on a subject’s friends and relations (Waddell, 2016). Critically, a person’s network is not a protected class, so while it may be illegal for an employer or lender to discriminate based on race, gender, or ability, it’s not illegal to discriminate based on algorithmic assumptions made that are in turn based on a person’s network (Boyd et al., 2014). Consider how much more of your network is documented and searchable now than ever before; your connection to a person the lender sees as undesirable is no longer theoretical or circumstantial, but instead comes with a lengthy data trail. Even though the realities of the people within a network may well be framed and circumscribed by those protected factors, nothing protects marginalized users from having this data turned against them. Which is to say: isn’t this just a fancy way to get around traditionally racist and classist practices?

Contract cheating firms are very aware of the power of algorithms—it’s how they find their clients. In Thomas Lancaster’s work describing how social media is used by contract cheating firms, he’s effectively describing an algorithmic process when he reflects on how “A single tweet by a student, even one expressing that they have an assignment due with no indication that they plan to cheat, can lead to them receiving 20 or more visible replies from contract cheating providers within an hour from when the tweet is made” (Lancaster, 2019b). These aren’t human beings scanning social media: these are bots. They phish for students in incredibly predatory ways, using algorithmic processing of key words to track students on social media and pounce when they are most vulnerable. If your institution has a hashtag it uses to collect student posts on social media, you can see this for yourself by following it for a little while, especially around midterms and finals. You’ll quickly find these companies using institutional hashtags to reach students, often cloaking their services in terms of “editing” or “tutoring” or “help.” It’s easy, especially if you’re not versed in institutional branding—or you’re just panicked and looking for any lifeline, and wanting it to be real—to see some of these posts and wonder if they’re legitimately

connected to the institution itself. And the companies also use these hashtags to track students as potential customers. They particularly like to use combinations of hashtags that pair a specific institution with words expressing affective experiences of student stress: #essaydue #finalsstress #essayhelp. So a student who is looking to commiserate with classmates on Instagram who uses the hashtag for her institution and, maybe, #freakingout #paperdue #needhelp, sends a bat signal not only for her classmates, but also for predatory contract cheating firms who sweep in to her direct messages at the last moment and offer “assistance.”⁴

While it is never okay to purchase an essay, it’s easy to imagine a situation where desperation combined with opportunity results in an individual making a choice they shouldn’t. Given the spiralling rise in contract cheating, it doesn’t seem likely that students are suddenly less ethical than they used to be, and research suggests that cheating is a highly contextual act, and even those students who seem to be predisposed to contract cheating typically do not engage in it for every assessment (Ramberg & Modin, 2019; Rundle et al., 2019). Students are targeted by predatory companies when they are at their most panicked and most stressed out, and it’s a form of quote-unquote “help” that they can access when they are at that lowest point—say, 2 am the morning before a paper is due—when legitimate resources like learning centres and campus tutors and office hours aren’t available. Contract cheating is wrong. Preying on vulnerable students, and profiting off their misery, is more wrong.⁵

Solutions

The barriers we place on learners, intentionally or not, can exacerbate the stakes and promote the fears and feelings that lead students to cheat. Whether it’s a high-cost homework system that leaves a student financially vulnerable, or inaccessible technology that can’t be accessed easily for students without stable internet connections, or a classroom environment that doesn’t allow students to adapt content for their own learning, all of these unnecessary barriers impede the ability of a student to succeed in a course. Each barrier brings additional stress. These barriers can also damage the relationship between faculty and student—and this relationship, too, has

⁴ In advance of Academic Integrity Day, we collected a large number of examples of these targeted ads in order to share the power of this imagery with our community. They have been archived with other artifacts from the day; see BC Academic Integrity Network in the references. Research in this area also includes Hersey, C. (2019). “*The struggle is real!*” #*Needapaperfast*. Paper presented at the Canadian Symposium on Academic Integrity, Calgary, Canada.

⁵ This is an aside, but many for-profit EdTech companies prey on faculty at their most vulnerable moments, too, making inquiries at the beginning and end of semester when tensions are highest and demands are many. As the precarity of the academic workforce increases and demands on instructor time do, too, this practice is only on the rise. These pitches invariably promise miraculous time-saving measures or huge improvements in student engagement. And they come directly to faculty rather than to an office of educational technologies or faculty development, which might mean they encounter less resistance or fewer questions.

an insulating effect on student rates of cheating (Orosz et al., 2015). When students feel responsible to a class and valued by their instructor, they cheat less.

Many other writers in this collection will point to what we know about pedagogical strategy for reducing the temptation to cheat: scaffolded assignments, low-stakes practice, and reducing anxiety around performance. The research shows that these strategies work. We know that students are more likely to cheat on high stakes assignments where they have received little guidance. Conveniently, we also know that those same kinds of assignments do little to promote meaningful learning. Research suggests that we can both promote learning and reduce stress and anxiety for students by scaffolding assignments appropriately, checking in at multiple stages, and providing opportunities for questions and feedback (Rundle et al., 2019). Authentic assessments, too, that students can see reflect clearly the expectations of the world outside the university, have a meaningful impact in terms of lowering rates of academic dishonesty (Medway et al., 2018). In truth, the tools we know work for good instruction work to reduce the temptation for engaging a contract cheating company in the first place (ICAI, 2016).

I propose we can compound the efficacy of these pedagogical interventions by helping students understand the value of their data and privacy, and modeling our respect for it in the way we use theirs: give students a full understanding of why their data has value, and then don't sell it out to the highest bidder on their behalf and without their informed consent. Does everyone understand the seriousness of handing over your SIN, or the responsibility to other people in your classes inherent to keeping your login information secure? In this case, not sharing is caring: we protect ourselves and each other when we keep our learning tools secure. And it's worth talking about how we secure learning materials, as well. Textbook question banks and homework system assignments are incredibly useful, time-saving tools for faculty members. They're also incredibly insecure. If you use a question bank produced by a textbook manufacturer or other third-party, I encourage you to do an experiment: take a random question from your bank and Google it. If that resource is remotely popular, it's likely that searching out that one question will bring up the entire question bank. While it's certainly true that some students will use test banks as study tools, it's also not a far skip to cheating—and be certain, contract cheating companies already have access to all of that content, too. When a lot of users are drawing on the same resource, it only takes one bad decision by one person to have all that material available on the open web. It's a good reason to invest in building these tools on-site, particular to each unique context.

Conclusions

It may seem like an extreme leap to connect the dots from an efficiency practice like using anti-plagiarism software or class-in-a-box courseware systems to the nefarious rise of contract cheating within our institutions. But what do we really mean when we assert a commitment to a culture of academic integrity? Is it acting with integrity

to allow student data to be monetized without compensation or to require students to subscribe to expensive services to submit assignments? Is it acting with integrity to offer no meaningful opt-out from or true informed consent for the use of these tools? And to return to that question from a student union representative at Academic Integrity Day, what do we model when it comes to the value of original work when institutional pressures like large class sizes and insufficient prep time lead us to lean on expensive—and, from an academic integrity perspective—wildly insecure tool like a homework system? We are responsible for modelling for our students what it looks like to be a contributing member of an academic community, and we do so by taking seriously our students, their data, and their work, and not only when it comes time to run it through a plagiarism detector or check their IDs against a proctoring software. When institutions serve students “course-in-a-box” content solutions; require them to engage with third-party, for-profit entities to submit their assignments; treat their data as valueless while someone else earns a profit; and sign away their rights to critique tools they are forced to use, we do not model academic integrity. Instead, we demonstrate that their education has been commodified, with each component bought and sold by interested parties.

To return to the words of the student union representative: if an instructor works within institutional pressures so egregious that the reasonable solution is to buy the lectures and assessments—and charge the student a premium for the experience—we lose the moral ground to say they cannot buy their submissions in turn. Academic integrity collapses when we fail to uphold our moral and ethical obligations, long before a student chooses to cheat.

References

- American Association of University Professors. (n.d.). *Primer on Privatization*. One Faculty, One Resistance. https://www.aaup.org/sites/default/files/Primer_on_Privatization%20%281%29.pdf
- BC Academic Integrity Network. (2019). Academic integrity day memes. *BC Academic Integrity Day*. <https://tru.arcabc.ca/islandora/object/tru:4954>
- Boyd, D., Levy, K., & Marwick, A. (2014). The networked nature of algorithmic discrimination. *Data and Discrimination: Collected Essays*. Open Technology Institute. <http://www.danah.org/papers/2014/DataDiscrimination.pdf>
- Cadloff, E. B. (2018, April 4). How do you solve a problem like contract cheating? *University Affairs*. <https://www.universityaffairs.ca/news/news-article/solve-problem-like-contract-cheating/>
- Christensen Hughes, J. (2017). *Understanding academic misconduct: Creating robust cultures of integrity*. Paper presented at the University of Calgary, Calgary. <http://hdl.handle.net/1880/110083>
- Clarke, R., & Lancaster, T. (2006). *Eliminating the successor to plagiarism: Identifying the usage of contract cheating sites*. Paper presented at the Second International Plagiarism Conference, Gateshead, UK. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.120.5440&rep=rep1&type=pdf>
- Eaton, S. E. (2020, January 15). Cheating may be under-reported across Canada’s universities and colleges. *The Conversation*. <http://theconversation.com/cheating-may-be-under-reported-across-canadas-universities-and-colleges-129292>

- Ellis, C., Zucker I.M., & Randall D. (2018). The infernal business of contract cheating: understanding the business processes and models of academic custom writing sites. *International Journal for Educational Integrity*, 14. <https://doi.org/10.1007/s40979-017-0024-3>
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Publishing Group.
- Gilliard, C. (2017). Pedagogy and the Logic of Platforms. *Educause Review*, July/August 2017. <https://er.educause.edu/articles/2017/7/pedagogy-and-the-logic-of-platforms>
- Hargittai, E., & Marwick, A. (2016). What Can I Really Do? Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, 10(0), 21. <https://ijoc.org/index.php/ijoc/article/view/4655>
- Hendershott, A., Drinan, P., & Cross, M. (2000). Toward Enhancing a Culture of Academic Integrity. *Journal of Student Affairs Research and Practice*, 37(4), 270–281. <https://doi.org/10.2202/1949-6605.1119>
- Hill, K. (2012). How target figured out a teen girl was pregnant before her father did. *Forbes*. <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>
- Huq, A. (2019). racial equity in algorithmic criminal justice. *Duke Law Journal*, 68(6), 1043–1134. <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3972&context=dlj>
- International Center for Academic Integrity (ICAI). (2016). *Institutional Toolkit to Combat Contract Cheating*. <http://integrity.fiu.edu/pdfs/Contract%20Cheating.pdf>
- Lancaster, T. (2019a). Profiling the international academic ghost writers who are providing low-cost essays and assignments for the contract cheating industry. *Journal of Information, Communication and Ethics in Society*, 17(1), 72–86. <https://doi.org/10.1108/JICES-04-2018-0040>
- Lancaster, T. (2019b). Social Media Enabled Contract Cheating. *Canadian Perspectives on Academic Integrity*, 2(2), 7–24. <https://doi.org/10.11575/cpai.v2i2.68053>
- Luke, J. (2019, March 13). That's No Plagiarism Checker. *EconProph*. <https://econproph.com/2019/03/12/thats-no-plagiarism-checker/>
- Macfarlane, B., Zhang, J., & Pun, A. (2014). Academic integrity: A review of the literature. *Studies in Higher Education*, 39(2), 339–358. <https://doi.org/10.1080/0307079.2012.709495>
- Medway, D., Roper, S., & Gillooly, L. (2018). Contract cheating in UK higher education: A covert investigation of essay mills. *British Educational Research Journal*, 44(3), 393–418. <https://doi.org/10.1002/berj.3335>
- Morris, E. J. (2016). Academic Integrity Policy and Practice: Introduction. In T. Bretag (Ed.), *Handbook of Academic Integrity* (pp. 409–411). Singapore: Springer Singapore.
- Newton, P.M. (2018). How common is commercial contract cheating in higher education and is it increasing? A systematic review. *Frontiers in Education*. <https://doi.org/10.3389/feduc.2018.00067/full>
- Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464), 447–453. <https://doi.org/10.1126/science.aax2342>
- Office of Ed Tech. (2012). *Pearson—Education Datapalooza*. <https://www.youtube.com/watch?v=xgV9DssLsXg>
- Olson, P. (2019). Pearson Hack Exposed Details on Thousands of U.S. Students. *Wall Street Journal*. <https://www.wsj.com/articles/pearson-hack-exposed-details-on-thousands-of-u-s-students-11564619001>
- Orosz, G. et al. (2015). Teacher enthusiasm: a potential cure of academic cheating. *Frontiers in Psychology*, 6, 318. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4379758/>
- Peters, M., Boies, T., & Morin, S. (2019). Teaching academic integrity in Queen universities: roles professors adopt. *Frontiers in Education*. <https://doi.org/10.3389/feduc.2019.00099/full>
- Peterson, H. (2019, May 10). Millions of students are buying plagiarism-free essays for as little as \$13—And it's nearly impossible for teachers to prove. *Business Insider*. <https://www.businessinsider.com/students-buying-essays-impossible-to-prove-2019-5>

- Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon*, 9(5), 1–6. <https://doi.org/10.1108/10748120110424816>
- Purdy, J. P. (2005). Calling off the hounds: Technology and the visibility of plagiarism. *Pedagogy*, 5(2), 275–296. <https://muse.jhu.edu/article/182339>
- Ramberg, J. & Modin, B. (2019). School effectiveness and student cheating: Do students' grades and moral standards matter for this relationship? *Social Psychology of Education*, 22, 517–538. <https://doi.org/10.1007/s11218-019-09486-6>
- Rhineland, J. (2017). Top Hat—Software to be avoided. *Imaginary Blog*. (n.d.). Retrieved November 20, 2020, from <https://imaginary.ca/blog/2017/06/16/top-hat/>
- Rigby, D., et al. (2014). Contract cheating & the market in essays. *Journal of Economic Behaviour & Organization*, 111, 23–37. <https://doi.org/10.1016/j.jebo.2014.12.019>
- Robinson, J. A., & Glanzer, P. L. (2017). Building a Culture of Academic Integrity: What Students Perceive and Need. *College Student Journal*, 51(2), 209–221.
- Rowland, S., et al. (2017). Just turn to us: The persuasive features of contract cheating websites. *Assessment and Evaluation in Higher Education*, 43(4), 652–665. <https://doi.org/10.1080/02602938.2017.1391948>
- Rundle, K., Curtis, G.J., & Clare, J. (2019). Why students do not engage in contract cheating. *Frontiers in Psychology*. <https://doi.org/10.3389/fpsyg.2019.02229/full>
- Senack, E., Donoghue, R., O'Connor Grant, K. & Steen, K. (2016). *ACCESS DENIED: The new face of the textbook monopoly*. Student PRIGs. <https://studentpirgs.org/assets/uploads/archive/sites/student/files/reports/Access%20Denied%20-%20Final%20Report.pdf>
- Smith, E. (2012). The Digital Native Debate in Higher Education: A Comparative Analysis of Recent Literature. *Canadian Journal of Learning and Technology*, 38. <https://doi.org/10.1002/9781118326732.ch>
- Stewart, B. (2020, November 10). Why higher ed needs data ethics. *Inside Higher Ed*. <https://www.insidehighered.com/blogs/university-venus/why-higher-ed-needs-data-ethics>
- Stinson, C. (2020, February 6). *Algorithms are not Neutral: Bias in recommendation systems*. The Department of Philosophy and School of Computing Colloquium Series presents, Queen's University, Kingston. https://www.catherinestinson.ca/Files/Papers/Algorithms_are_not_Neutral.pdf
- Stommel, J., & Morris, S. M. (2017). A Guide for resisting edtech: The case against Turnitin. *Hybrid Pedagogy*. <https://hybridpedagogy.org/resisting-edtech/>
- Sutherland-Smith, W., & Dullaghan, K. (2019). You don't always get what you pay for: User experiences of engaging with contract cheating sites. *Assessment & Evaluation in Higher Education*, 44(8), 1148–1162. <https://doi.org/10.1080/02602938.2019.1576028>
- Swauger, S. (2020). Our bodies encoded: Algorithmic test proctoring in higher education. *Hybrid Pedagogy*. <https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/>
- UNESCO IITE. (2020). *Personal data security technical guide for online education platforms*. UNESCO. <https://iite.unesco.org/publications/personal-data-security-technical-guide-for-online-education-platforms/>
- Waddell, K. (2016, December 2). How algorithms can bring down minorities' credit scores. *The Atlantic*. <https://www.theatlantic.com/technology/archive/2016/12/how-algorithms-can-bring-down-minorities-credit-scores/509333/>
- Yorke, J., Sefcik, L., & Veeran-Colton, T. (2020). Contract cheating and blackmail: A risky business? *Studies in Higher Education*, 1–14. <https://doi.org/10.1080/03075079.2020.1730313>
- Zubairi, A. (2017, March 4). *CEO Mike Silagadze explains how data on Top Hat's platform can help struggling students*. Betakit. <https://betakit.com/ceo-mike-silagadze-explains-how-data-on-top-hats-platform-can-help-struggling-students/>
- Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. London: Profile Books.

Brenna Clarke Gray (MA Carleton, Ph.D. New Brunswick) is a literature scholar by training, a comics scholar by practice, and an educational technologist by trade. Her research interests include open pedagogies and ethical approaches to educational technologies. She is the Coordinator, Educational Technologies at Thompson Rivers University and is currently at work tracing the history and imagining the future of open tenure processes.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

