education policy analysis archives

A peer-reviewed, independent,
open access, multilingual journal

epaa aape

Arizona State University

Volume 30 Number 175 December 6, 2022 ISSN 1068-2341

AI, Biometric Analysis, and Emerging Cheating Detection Systems: The Engineering of Academic Integrity?

Jo Ann Oravec

University of Wisconsin-Whitewater, University of Wisconsin-Madison

United States

Citation: Oravec, J. (2022). AI, biometric analysis, and emerging cheating detection systems: The engineering of academic integrity? *Education Policy Analysis Archives, 30*(175). https://doi.org/10.14507/epaa.30.5765

Abstract: Cheating behaviors have been construed as a continuing and somewhat vexing issue for academic institutions as they increasingly conduct educational processes online and impose metrics on instructional evaluation. Research, development, and implementation initiatives on cheating detection have gained new dimensions in the advent of artificial intelligence (AI) applications; they have also engendered special challenges in terms of their social, ethical, and cultural implications. An assortment of commercial cheating–detection systems have been injected into educational contexts with little input on the part of relevant stakeholders. This paper expands several specific cases of how systems for the detection of cheating have recently been implemented in higher education institutions in the US and UK. It investigates how such vehicles as wearable technologies, eye scanning, and keystroke capturing are being used to collect the data used for anti-cheating initiatives, often involving systems that have not gone through rigorous testing and evaluation for their validity and potential educational impacts. The paper discusses accountability- and policy-related issues concerning the outsourcing of cheating detection in institutional settings in the light of these emerging technological practices as well as student resistance against the systems involved. The cheating-detection practices can place students in a disempowered, asymmetrical position that is often at substantial variance with their cultural backgrounds.

Journal website: http://epaa.asu.edu/ojs/
Facebook: /EPAAA
Twitter: @epaa_aape

Manuscript received: 7/20/2020
Revisions received: 6/21/2021
Accepted: 21/6/2021

Keywords: deception; surveillance; privacy; intellectual autonomy; academic cheating; higher education policy; accountability; artificial intelligence; facial recognition; biometrics

IA, análisis biométrico y sistemas emergentes de detección de trampas: ¿La ingeniería de la integridad académica?

Resumen: Los comportamientos de trampa se han interpretado como un problema continuo y un tanto molesto para las instituciones académicas, ya que cada vez realizan más procesos educativos en línea e imponen métricas en la evaluación de la instrucción. Las iniciativas de investigación, desarrollo e implementación sobre la detección de trampas han adquirido nuevas dimensiones con la llegada de las aplicaciones de inteligencia artificial (IA); también han generado desafíos especiales en términos de sus implicaciones sociales, éticas y culturales. Se ha inyectado una variedad de sistemas comerciales de detección de trampas en contextos educativos con poca participación por parte de las partes interesadas relevantes. Este artículo amplía varios casos específicos de cómo los sistemas para la detección de trampas se han implementado recientemente en instituciones de educación superior en los EE. UU. y el Reino Unido. Investiga cómo se utilizan vehículos como tecnologías portátiles, escaneo ocular y captura de pulsaciones de teclas para recopilar los datos utilizados para iniciativas contra las trampas, que a menudo involucran sistemas que no han pasado por pruebas y evaluaciones rigurosas para determinar su validez y posibles impactos educativos. El documento analiza cuestiones relacionadas con la rendición de cuentas y las políticas relacionadas con la subcontratación de la detección de trampas en entornos institucionales a la luz de estas prácticas tecnológicas emergentes, así como la resistencia de los estudiantes contra los sistemas involucrados. Las prácticas de detección de trampas pueden colocar a los estudiantes en una posición asimétrica y sin poder que a menudo difiere sustancialmente de sus antecedentes culturales.

Palabras clave: engaño; vigilancia; privacidad; autonomía intelectual; trampa académica; política de educación superior; *accountability*; inteligencia artificial; reconocimiento facial; biometría

IA, análise biométrica e sistemas emergentes de detecção de trapaça: A engenharia da integridade acadêmica?

Resumo: Os comportamentos de trapaça têm sido interpretados como um problema contínuo e um tanto irritante para as instituições acadêmicas, uma vez que cada vez mais conduzem processos educacionais online e impõem métricas na avaliação instrucional.Iniciativas de pesquisa, desenvolvimento e implementação de detecção de trapaça ganharam novas dimensões com o advento de aplicativos de inteligência artificial (IA); eles também geraram desafios especiais em termos de suas implicações sociais, éticas e culturais. Uma variedade de sistemas comerciais de detecção de trapaça foi injetada em contextos educacionais com pouca contribuição por parte das partes interessadas relevantes. Este artigo expande vários casos específicos de como os sistemas de detecção de trapaça foram recentemente implementados em instituições de ensino superior nos EUA e no Reino Unido. Ele investiga como veículos como tecnologias vestíveis, varredura ocular e captura de pressionamento de tecla estão sendo usados para coletar os dados usados para iniciativas antitrapaça, muitas vezes envolvendo sistemas que não passaram por testes e avaliações rigorosos quanto à sua validade e possíveis impactos educacionais. O artigo discute questões relacionadas à responsabilidade e políticas relacionadas à

terceirização da detecção de trapaça em ambientes institucionais à luz dessas práticas tecnológicas emergentes, bem como à resistência dos alunos contra os sistemas envolvidos. As práticas de detecção de trapaça podem colocar os alunos em uma posição desempoderada e assimétrica que muitas vezes está em desacordo substancial com suas origens culturais.
Palavras-chave: engano; vigilância; privacidade; autonomia intelectual; trapaça acadêmica; política de educação superior; *accountability*; inteligência artificial; reconhecimento facial; biometría

AI, Biometric Analysis, and Emerging Cheating Detection Systems: The Engineering of Academic Integrity?

Detection of cheating in student evaluation contexts has often been identified as one of the "ongoing issues" in academia (Pathak, 2016, p. 315). It has taken on special emphases as online, blended, hybrid, and other commodified education modes expand and "scandalous" levels of cheating are reportedly noted (Klein, 2020). As related in this paper, cheating and deception-detection initiatives have gained new dimensions in the advent of such artificial intelligence (AI) advances as personal profiling and facial recognition; they have also encountered special challenges in terms of potential bias, privacy concerns, and other negative personal and social impacts. For the past decades, some students have indeed engaged in cheating behaviors without the aid of technology, and faculty and staff members have proctored exams on a face-to-face basis. However, the deception-detection systems and practices described in this paper are often rooted in the outsourcing of basic institutional functions to third-party developers and implementers, as well as involve technologies such as AI-enabled profiling in which substantial aspects are opaque to the subjects (Andrejevic & Selwyn, 2019; Oravec, 2022; Zeng et al., 2019). Many important questions concerning the systems' operations are largely unanswered for the students, faculty, and staff who are a part of these initiatives, from issues of "algorithmic accountability" (Hoffmann, 2019) to how resulting data are disseminated. Also emerging in the academic cheating picture are corporate entities that actively and openly offer contract cheating services and paper mill products to students online, providing a confusing mix of powerful technological and institutional influences for organizational participants to decipher.

The technological "arms race" that involves corporate cheating detection system developers, cheating assistance purveyors, and technology-savvy student participants is attracting increased attention to cheating as an institutional issue as well as generating iterations of technological developments. This paper focuses on academic cheating in the context of the US and UK, but many other nations have faced comparable cheating issues (Costley, 2019; Denisova-Schmidt et al., 2016; Pan et al., 2019; Song-Turner, 2008), and many of the specific technological cheating-detection systems described have had international reach.

Cheating and Deception Behaviors

Kinds of behavior construed as "academic cheating" vary widely, and their iterations can add new dimensions to the moral ecologies of colleges and universities. These include plagiarism (Zhang, 2016), collusion (collaboration on assignments or examinations that is not approved by the instructor), and use of services that complete courses for a student (Malesky Jr. et al., 2016), as well as less intentional phenomena such as cryptomnesia and inadvertent self-plagiarism (Dow, 2015).

Lipson and Karthikeyan (2016) describe a broad set of "innovative mechanisms and insidious ploys in academic deceit" (p. 48). For example, cheating sometimes involves instructors or staff members playing direct roles in altering the scores of certain individuals (Turner, 2016).

Impersonation is also a part of the cheating realm, as students or paid professionals complete assignments or take exams for each other. Not long ago, the notion of a student impersonating another student in order to take an exam was indeed a possibility, but was relatively rare (Moeck, 2002). However, impersonation has become a serious issue for universities implementing online programs. In response to these concerns, Berkey and Halfond (2015) state that "An online program cannot claim to be truly worthy of academic recognition without strong assurance that students are being fairly and effectively assessed in their learning" (p. 1). In many institutions, individuals may obtain academic degrees without setting foot on a particular campus or meeting face-to-face with instructors, often increasing expressions of concern by administrators about student identity manipulations (Boafo-Arthur & Brown, 2017; Song-Turner, 2008).

Student impersonation detection has engendered considerable problems in many institutions, especially those that legally require the authentication of student attendance (Kaiser & Hogan, 2010; Whitten, 2017). In the US, requirements for the authentication of student attendance are often linked to the potentials for financial aid fraud as some individuals reportedly simulate participation in order to claim student loans (Owen, 2016). Many educators have projected that if higher education institutions are to fulfill their aims of reaching thousands of students throughout the globe for instructional and assessment purposes, online education programs will require some form of large-scale implementation of personal authentication systems to certify attendance and prevent impersonation (Liyanagunawardena et al., 2013; Vegendla & Sindre, 2019).

"Contract cheating" is another academic cheating variant. Forms of contract cheating have been around for decades, but the widespread presence of organizations that are open purveyors of academic papers and even online course completions is more recent (Sutherland-Smith & Dullaghan, 2019). The normalization of such practices in many contexts has created difficult issues for higher education institutions (Ćerimagić & Hasan, 2019; Stoesz et al., 2019). The excerpt below from a study of contract cheating shows its effectiveness in deceiving faculty:

> Websites now advertise the service of taking online courses for students… Representatives from the company were professional and delivered the advertised services. Two experienced faculty members who co-taught the course used in this study were unable to identify the cheating company. The cheating company earned an "A" for the student. (Malesky Jr. et al., 2016, p. 178)

Although the description above casts these contract cheating services as being successful in deception efforts, other characterizations outline how the services can often produce inferior products that can expose students to blackmail attempts (Sutherland-Smith & Dullaghan, 2019; Yorke et al., 2020). Policies that academic institutions develop about cheating detection efforts should recognize the growing presence and visibility of these services and their psychological impact on students, many of whom are very aware of their peers using them to gain perceived advantages (Amigud & Dawson, 2020).

The Emergence of the Deception-Detection Industry

In past centuries, the prospects of being monitored and detected in their efforts to elude the gaze of a human proctor or invigilator often served as a deterrent for students; however, technologically-supported platforms have replaced many traditional examination settings in the past

several decades (Harding, 2018). Academic institutions have implemented a wide range of different technological anti-cheating systems; for instance, anti-plagiarism systems such as *Turnitin* have been used in educational institutions since the 1990s and have generated substantial case law as to their appropriate applications (Introna, 2016; Vanacker, 2011).

Few higher education institutions have their own homegrown systems of online cheating detection, although individual faculty members or departments may indeed have developed something for their own specialized uses. Cheating detection is among the many aspects of higher education that have been heavily outsourced to corporations, with associated concerns about how the corporations involved are handling privacy and security issues. There are growing genres of systems that are licensed by higher education institutions and integrated into learning management systems (LMS), with names such as *ProctorU*, *Proctortrack*, and *Examity* (Kolowich, 2013; Singer, 2015) as well as *Proctorio* (OReilly & Creagh, 2016). Some of the other forms of online deception also have systems that are specially tailored for the context, with several focusing specifically on student impersonation challenges.

Since the technology developers of cheating-related approaches are generally third-party organizations not directly affiliated with educational institutions, they may construe themselves as not being bound by specific institutional constraints and student welfare concerns. Examples include *Examity*'s live proctoring option, described here by a journalist:

> Hayes was required to upload a picture of his photo ID to *Examity*'s website and provide his full name, email, and phone number — pretty banal stuff. But it got weirder. At the end, he typed his name again; *Examity* would store a biometric template of his keystrokes… Hayes was preparing to take his first practice exam, with an *Examity* proctor watching him over Zoom… Sharath [the *Examity* proctor] told Hayes to share his screen, and then to display both sides of his driver's license in the webcam's view. "I need to see your desk and workspace," the proctor said. "Please rotate your webcam 360 degrees so I can see the area around you." Hayes complied. "Please take a step back and show me the entire desk," the proctor instructed. Again, Hayes obeyed… The proctor entered a password, using Hayes' computer, and the test — taken online through *Examity*'s portal — began. Sharath watched Hayes work, through his webcam, the entire time. (Chin, 2020, para. 5-8)

Methods to detect cheating have expanded as technological capabilities increase (Perry-Hazan & Birnhack, 2016). For example, drones have been used in cheating-detection efforts in some universities to hover over the heads of students (Demetriou, 2015; Grym & Liljander, 2016). The methods used include some technological approaches that may appear to be intrusive in the context of educational evaluation, such as webcams that record students' bodily expressions during exams (Blair et al., 2015) or keystroke analyzers (Byun et a., 2020). Wearable technologies have also been used that collect medical information that can be decomposed into "stress level" indicators, with physical indices of stress often linked to cheating behaviors. For example, Fort, Raymond, and Shackelford (2016) portray the recent use of wearable technologies as an "angel on our shoulder" for a growing number of individuals in institutional settings, recording various physiological indicators, conducting analyses, and providing certain stimuli in response. Some systems for cheating detection are integrating machine learning capabilities, engaging in large-scale testing and analysis on students that often involves the construction of personal profiles. Coherent institutional policies involving the growing range of AI-enhanced proctoring and identity-verification technologies have been very slow to surface in an arena that has critical importance to academic culture and student wellbeing (Burgason et al., 2019; Burke & Bristor, 2017; Shams, 2017).

Some Ethical Dimensions of Cheating Detection Systems

In past centuries, various inhumane tests were applied in certain circumstances in order to ascertain whether individuals were telling the truth when asked whether they were indeed prevaricating (Florczak & Wujczyk, 2020; Underwood, 1995); these ordeals often included rough interrogation and torture. The technology-enhanced practices that are currently involved in catching cheaters and detecting deception may be more sophisticated and less bizarre than these previous practices, but can still leave individuals with the responsibility to demonstrate that they were not attempting to deceive, a difficult thing to do especially when facing complex technological systems. Constructions of suspect cheating behavior can differ among the various proprietary and in-house anti-cheating systems (with some emphasizing eye movements and others head or hand gestures), possibly resulting in anxieties and cognitive dissonance in students as well as confusions for faculty and staff who are called upon to interpret these phenomena. Many of the facial expressions and various gesticulations associated with cheating are related to intimate personal expression involving decision making; influencing these expressions by imposing high tech surveillance could lead to disruption of the subjects' deliberations.

Cultural differences or past experiences with institutional administrations and law enforcement can affect students' interpretations of deception-detection and related surveillance practices, especially the practices involving facial and hand gestures (Bygrave & Aşık, 2019). The contexts of online proctoring often introduce special complications and challenges for certain students. For example, students who face external distractions in their home environments or illnesses may be classified as suspects. Unfortunately, since students are often not given the opportunity to explain what transpired in their particular household settings, data that portrays them as being potential cheaters can still be a part of various organizational databases whatever the outcomes of a specific charge against them. The "digital divide" itself can be a factor, with students not given equitable technological access and training, which can result in problematic use of educational systems. The prospects are frightening for lists of "potential cheaters" being compiled and made available for later, unspecified use; such stigma-associated data could be used in future decision-making contexts in employment and civic arenas (Hoffmann, 2019).

Students who are obligated to utilize cheating-detection systems are often faced with invasive home, technological, and personal requirements. Consider the following scenario from a recent journalistic source, rooted in the kinds of systems described in this paper:

> When student Marium Raza learned that her online biochemistry exam at the University of Washington would have a digital proctor, she wanted to do her research. The system, provided by a service called Proctorio, would rely on artificial intelligence and a webcam to monitor her while she worked…"We don't have any transparency about how our recorded video is going to be used or who is going to see it," Raza told Recode. "The status quo should not be visualizing each student as someone who is trying to cheat in any way possible." Raza wasn't the only one in her class who felt concerned about new levels of surveillance... Worse, the tool's facial detection algorithm seemed to struggle to recognize them, so they needed to sit in the full light of the window to better expose the contours of their face, in their view an indication that the system might be biased. (Heilweil, 2020, para. 1-3)

As characterized above, cheating-detection practices can place students in a disempowered, asymmetrical position, one that is often at variance with students' cultural backgrounds. The

challenges in defending against allegations of cheating could be intensified by the students' lack of economic resources and institutional savvy. The coupling of artificial intelligence approaches with cheating-detection systems can increase the apparent effectiveness and rhetorical power of the systems and can make countering the systems' results even more difficult for those accused of cheating.

The numbers of narratives about the physical and social indignities involved with deception-detection systems are growing, along with their disseminations in popular and social media. These scenarios can be demoralizing, degrading, and filled with uncertainty, whether or not there is a human proctor in the mix:

> When University of Florida sophomore Cheyenne Keating felt a rush of nausea a few weeks ago during her at-home statistics exam, she looked into her webcam and asked the stranger on the other side: Is it okay to throw up at my desk?
>
> He said yes. So halfway through the two-hour test, during which her every movement was scrutinized for cheating and no bathroom breaks were permitted, she vomited into a wicker basket, dabbed the mess with a blanket and got right back to work. The stranger saw everything. When the test was finished, he said she was free to log off. Only then could she clean herself up… Looking off-screen for too long, for instance, can raise a test-taker's "suspicion" score, potentially leading them to fail the exam. (Harwell, 2020, para. 1-3)

Students can be labeled as probable violators of integrity rules, whether or not they are aware of exactly what went into the trigger. This could be upsetting enough: but, what are the rules that were violated? What was the mix of characteristics and behaviors that triggered the alarm? The notion that the algorithms involved in the production of identity scores are proprietary and effectively off-limits to anyone without court assistance is deeply embedded in corporate-managed cheating and deception contexts. The ethical asymmetries involved in this arrangement complicate its use for mitigating cheating. The traditional forms of dealing with cheating (for example, with human proctors) were at least moderately transparent, albeit often idiosyncratic in their own ways. It is indeed impossible to prove beyond a doubt that someone is guilty or innocent; confessions often make the difference in hearings on academic deception matters. Learning how to look like a "person of integrity" (and passing as an innocent individual) is part of the implicit instruction that is involved in human-system as well as human-human interaction, with individuals ascertaining the sorts of movements and expressions associated with honesty. If automated, third-party systems are utilized, clear understandings of how the systems are intended to work as well as statistics as to how they actually operate in practice should be available to stakeholders, including students.

Students as Assumed Deceivers

It is generally considered to be in the best interest of students to participate in academic programs with high reputations, in which their future employers or colleagues can trust that they and their fellow students completed their courses successfully and with integrity (Chapman & Lindner, 2016). However, basic information about the use of cheating-detection mechanisms is generally not provided to students, even though schools are obligated to produce lengthy and detailed reporting on security issues and on-campus violence. Many academic conduct policies are often unclear and possibly even intentionally ambiguous, leaving faculty with some discretion in individual cases (Zamastil, 2004). Some of the systems discussed in this paper in effect portray the student in terms of the degree of potential cheating; every student is considered a little bit in violation of "integrity,"

perhaps for looking down once too often at something on his or her desk and staring at the ceiling. Consider the following scenario from a university newspaper:

> On Nov. 11, a student received an email from his Fundamentals of Computer Science 1 professor that sent a wave of panic through his body. "You have been found to be in violation of the course academic integrity policy on the following assignment(s) in CS2500," the email read. Another student had copied his code and both had been reported to the Office of Student Conduct and Conflict Resolution, or OSCCR, for plagiarism. "I helped someone out and that person just decided to copy word for word. Now we're both in this situation," he said. The second-year computer science and computer engineering combined major, who requested anonymity citing fear of professional consequences, wasn't alone. Over 100 students in the class… received the same email for various types of plagiarism…. (Angulo, 2019, para. 1-5)

Impacts of the "cheating" designation are indeed severe; students who are interviewed concerning the possibility of cheating and who are able to defend themselves can face a loss of morale. Students who confess to cheating or who are formally designated as cheaters without their confessions can face continuing academic and social struggles.

Since the ramifications of being labeled as potential cheaters may be severe for individuals, conscientious attention to the social and ethical issues involved is imperative for system researchers, developers, and implementers (Majeed et al., 2017; Oravec, 2020; Taylor, 2013). However, the basic reliability and validity of these systems in higher education contexts are in question (Majeed et al., 2017), with relatively few assessment efforts underway. The amount of data collected in cheating detection systems can be substantial and the students often ill-equipped to mount substantial administrative or legal challenges, whether or not the resultant analyses are needed or appropriate. The use of integrity scores as tools for the ranking of the relative levels of compliance of students opens the door to bias and opportunism, especially when the context of the scores, relative rankings among students, and other information are not provided. What complicates the analysis and testing of these cheating-detection systems is that cheating can rarely be "proven": often, the admission of guilt on the part of students who are faced with some amount of evidence is what ends the case in question. Students may unintentionally provide some physical clues as to their intention to deceive, often known as "leakage" (Verplaetse et al., 2007), though these expressions (such as profuse sweating) are not conclusive in establishing guilt. Relatively few cases of academic cheating go as far as a formal legal hearing (institutional administrative hearings are more common), so precedent in terms of what would be acceptable is quite sparse in comparison with some employment contexts.

Deception-detection organizations have so far faced little legal and social opposition, with practices that are potentially problematic in terms of privacy and bias. In a comparable context, educational testing organizations have often been treated kindly by the courts, with limited restrictions on what they can do in their efforts to create credible testing systems. For example, the Educational Testing Service (ETS) has generally been supported in its attempts to invalidate the test scores of individuals or groups it deems are cheating in some way (Semko & Hunt, 2013). The plagiarism-detection program Turnitin has successfully fought hundreds of legal attacks for its apparent usurpation of student copyrights and other supposed affronts (Muriel-Torrado & Fernández-Molina, 2015). These organizations have often served as "outsourcers" for the purposes of anti-cheating system development and administration, deflecting some of the concern that inherent system biases could be exposed and the university administrations put at risk. The anti-deception systems cannot be fully "tested" themselves—there is no way to prove that a glance at a

smartphone was directly related to some sort of inappropriately-aided intellectual outcome. Students are indeed nearly helpless in fighting high tech organizations that have only an outsourcing relationship with the higher education institution as a whole. Even if a ruling against the particular practices would be put into place, new practices would evolve and different organizations would take on the institution's anti-cheating agendas.

Resistance to Cheating Detection Systems

Requiring compliance to newly-instituted, potentially-problematic systems at the price of derailing one's own academic future is a tough request to make of students, whatever the demands placed on institutions in regard to cheating detection. With sufficient effort, institutions can indeed implement humane and transparent ways of dealing with cheating and deception issues. Coherent policies on the part of higher education institutions about the kinds and extents of cheating-detection efforts are often lacking, a situation that is comparable to other high tech and software concerns such as information security (Slade et al., 2019; Weidman & Grossklags, 2018).

Reasons for students to resist these anti-deception systems in this pre-policy era are increasing. Accounts such as the following in the *New York Times* are capturing the response of some students to what is happening:

> As Daniel Farzannekou prepared to take an online exam late last month in his naval science elective at the University of California, Los Angeles, the software directed him to pick up his laptop and scan his room, his desk, his ID and his face. "Ridiculous," Mr. Farzannekou, a 20-year-old history major, fumed. He grabbed a notepad from his girlfriend, scribbled a two-word profanity in black ink and pointedly held it up to the webcam. Then he uninstalled the digital proctor software and fired off an email to his professor. The monitoring system was like something out of "communist Russia," he wrote, demanding a less Orwellian test. (Hubler, 2020, para. 1-2)

Few students have the means to challenge the testing context in the way just described. In response to such a situation, students could choose not to patronize certain educational establishments, taking the approach of a number of households that removed their children from high stakes testing (Kempf, 2016). Some students have worked to make face-to-face proctoring a viable option (such as at Rutgers University in the US), though at an extra fee (Singer, 2015). The underpinnings for a class-action approach for those negatively affected would take years to put into place, and system-related harm would need to be identified and possibly monetized as well. The resources needed to analyze the considerable amount of data pertaining to the deception-detection system in question and how it was utilized over time in an institutional context provide foreboding obstacles to those who would seek to litigate or work with various governmental agencies to document bias, unfairness, or inhumanity.

Resistance can take a number of forms beyond the legal maneuvers just described. The technological escalation that occurs when students share tips online as to how to work around certain surveillance features can foment a kind of gamesmanship that can run counter to academic values of integrity and trust, whatever their justification. These escalation patterns can be iterative and may not have an apparent conclusion (Oravec, 2015, 2022). Cheating and its detection can be considered as an arms race in which particular technological advances for detectors are often matched with advances by those who are under surveillance (Lipson & Karthikeyan, 2016). The crowdsourcings of subjects' reflections about some of the cheating-deception systems in place are

already being used by students and employees to alter their behavior in various testing and evaluation contexts (as described in Rozario, 2020). Although it is generally construed in negative terms, cheating can often be well characterized as "subversive and strategic resistance" to stifling and oppressive systems (Högberg, 2011), in much the same way some impoverished individuals reportedly enact resistance by deceiving those who administer anti-poverty programs (Madden, Gilman, Levy, & Marwick, 2017) and incarcerated individuals use deception to gain small advantages in prison (Lingel & Sinnreich, 2016).

Preventive and proactive efforts to provide assistance to students who are "at risk for being reported for cheating" (Gallant, Binkin, & Donohue, 2015) may serve a better social purpose than "catching" apparently nonconforming students and subsequently punishing or expelling them. Educational institutions along with other forms of organizations impart lessons to their participants about their moral and social statuses in the world, including their roles as consumers of educational products and subjects of surveillance (Oravec, 2017; Tomlinson, 2016). The context of examinations is especially relevant in the ways it prepares young people to accept surveillance practices in their future workplace or school contexts. Unfairness and inappropriate adaptation of these electronic tools could indeed groom students for their future employment-related lives encountering systems that are themselves unfair and opportunistic. Since cheating detection is only one aspect of the broader set of privacy-related concerns individuals have to deal with, "privacy fatigue" could become a factor in the level of student resistance (Choi et al., 2018, p. 42); individuals' responses could be dampened because of the overwhelming extent of surveillance and monitoring concerns in their households, workplaces, and communities.

Future Directions and Implications for Educational Policy

Academic cheating- and deception-detection initiatives present disconcerting potentials as they are coupled with artificial intelligence, biometrics, and facial recognition methodologies. For instance, some research currently being done on deception integrates detailed information about individuals' biometric indicators and other personalized data in search of individualized patterns of signals about their deception-related intentions (Tonguç & Ozkara, 2020; Traoré et al., 2017). The data that result from such initiatives may be stored and used over time as ways to ascertain whether the individuals are indeed conforming to particular standards of integrity in various contexts. For instance, lists of subjects who are construed as "potential cheaters" as a result of their interactions with the cheating-related systems could be compiled; predictive analytics could subsequently be used to project the individuals' future activities (Sprague, 2015; Verplaetse et al., 2007). The notion that using AI is somehow "fairer" than face-to-face human proctoring (as proposed in Daugherty et al., 2019) needs to be examined systematically over time, along with other assumptions about the superiority of AI-enhanced processes. The algorithms undergirding the system and the generation of "integrity scores" (Tene & Polonetsky, 2013) are generally proprietary and inaccessible to those using the system, which makes the system a form of "black box."

Technological futures for deception-detection technologies include the possibility of neuroscientific systems for scanning individuals' brains to ascertain their levels of conformity (Blitz, 2016; Zeng et al., 2019). These systems could have long-term impacts on subjects' ethical thinking and related behavioral expression, for instance severing the linkages between thought and certain forms of facial movement. If individuals are given little or no feedback as to what kinds of "leakage" or "tells" supposedly signal their current or planned deceptions they could minimize or exaggerate certain kinds or levels of emotional responses in general or engage in the kinds of expressive repertoire recommended in their crowdsourcing efforts. False positives are certainly to be expected,

forcing individuals to prove that they were not cheating, efforts that can be demoralizing and debilitating. Even more troubling are prospects for experimentation with the systems on the part of the researchers, developers, and implementers involved, for example, providing false feedback to subjects with the aim of testing the systems or enhancing subjects' responses. Systematic, machine-monitored rewarding of inauthentic responses over time can present unsettling prospects for mental health as well as societal and ethical norms.

Many individuals are being surveilled from birth with technologies that include crib monitors, interactive toys, and wearable computing (Fort et al., 2016); they are also increasingly learning through their interactions with deception detection systems and related surveillance technologies what the systems construe as "acceptable" in terms of behavior (Burgason et al., 2019). Construction of integrity scores for individuals provides the potentials for individuals' lifetime identification with cheating, although the scoring may be construed by system developers as somehow personalizing the systems and increasing their validity. Many of the current practices relating to anti-cheating efforts place cheating as largely a behavioral issue, akin to drug testing practices in sports; false positives that occur in the systems are often construed as collateral damage by those whose primary focus is punishing violators (Ćerimagić & Hasan, 2019; Moston & Engelberg, 2019). Asymmetries of power in this regard can make the processes of catching student cheaters largely ones of intimidation, using something that appears to be a sophisticated, high-tech system framed in moralistic rhetoric. The use of the phrase "compliance scores" (Kaiser & Hogan, 2010) rather than "integrity scores" would be one step toward putting the systems' results in another, less moralistic perspective, although the notion of compliance could have other, disempowering implications. There are other ways of dealing with cheating: academic institutions that facilitate reflective and culturally-sensitive practices to counter cheating impart different values to students than those that impose poorly-tested online surveillance systems (Dalal, 2019, p. 175).

Conclusions and Reflections

AI applications in cheating detection systems have the potential to change radically the relationships among students, faculty, staff, and their organizations, perhaps reducing the documented occurrences of cheating in some settings but also introducing new possibilities for bias and personal disempowerment. Few higher education institutions are undertaking methodical evaluations of the accountability of the systems' developers, providers, and administrators: the technologies involved are often being used in academic contexts with little scientific justification for their efficacy or systematic examination of their fairness. Often by the time evaluations can be assembled, new technologies are made available and put into place, also without adequate examination. Institutional policies have provided students and faculty with only minimal guidance as to the privacy and fairness factors involved, with the status of the technologies in question as generally third-party and proprietary as an obstacle. With this lack of policy guidance, students who enter a higher and further education institution intending to complete a multi-year program generally cannot expect to have assurances as to what kind of proctoring and online surveillance strategy will be utilized during their educational efforts, with such information generally being released when they receive the syllabi for particular courses.

Accusations of cheating can be devastating for students and very hard to defend against with some cheating-detection systems. Challenges in defending against technologically generated allegations of cheating (with assumptions of being deemed guilty before having a chance to be proven innocent) could diminish the position of the student as a moral agent. There may indeed be differential impact in some of the cheating detection technologies discussed in this paper, with

special dangers associated with certain groups (such as individuals with identified disabilities or certain racial or ethnic affiliations) suffering disproportionately negative consequences. However, determining and possibly mitigating these consequences in a systematic way will require dedication and resources. There would need to be a cheating detection system in place long enough to do the required analyses as well as motivated individuals who are focused on challenging the negative impacts. The prospects for experimentation and entrapment in systems implementation are also frightening, and given the fact that many of the systems are largely run by third-party outsourcers such prospects are considerable. The notion that fairness is more achievable in machine-driven deception-detection systems than in situations in which humans do face-to-face monitoring can run counter to the more realistic perspective that various biases can be inherent in system algorithms and that false positives are likely (especially in the early stages of system operation).

The focus placed in educational institutions on the authenticity of exam participation and the credibility of results makes the technological practices discussed in this paper resilient and difficult to challenge for concerned participants. Faculty and staff members can work to diminish the temptation to conflate student conformity with the system's basic requirements as any sort of expression of "honor" or "integrity." Being accused of cheating or deception and not being able to defend oneself or even fully to understand the context is disempowering for individuals and runs counter to academic values of transparency and openness. Critical examinations of the ethical and legal dimensions of anti-cheating systems may help to expose system limitations and the potential dangers to essential civil liberties.

References

Amigud, A., & Dawson, P. (2020). The law and the outlaw: Is legal prohibition a viable solution to the contract cheating problem? *Assessment & Evaluation in Higher Education, 45*(1), 98-108. https://doi.org/10.1080/02602938.2019.1612851

Andrejevic, M., & Selwyn, N. (2019). Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology, 45*(2), 115-128. https://doi.org/10.1080/17439884.2020.1686014

Angulo, I. (2019, December 4). Plagiarism controversy brings cheating culture in 'Fundies' to light. *The Huntington News* (Northeastern University). https://huntnewsnu.com/61093/campus/plagiarism-controversy-brings-cheating-culture-in-fundies-to-light/

Beckman, T., Lam, H., & Khare, A. (2017). Learning assessment must change in a world of digital "cheats." In *Phantom ex machina* (pp. 211-222). Springer International Publishing. https://doi.org/10.1007/978-3-319-44468-0_14

Berkey, D., & Halfond, J. (2015). Cheating, student authentication and proctoring in online programs. *New England Journal of Higher Education,* (Summer). https://nebhe.org/journal/cheating-student-authentication-and-proctoring-in-online-programs/

Blair, J. P., Levine, T. R., & Vasquez, B. E. (2015). Producing deception detection expertise. *Policing: An International Journal of Police Strategies & Management, 38*(1), 71-85. https://doi.org/10.1108/PIJPSM-09-2014-0092

Blitz, M. J. (2016). The Fourth (and First) Amendment: Searches with, and scrutiny of, neuroimaging. In *Searching minds by scanning brains* (pp. 81-123). Springer. https://doi.org/10.1007/978-3-319-50004-1_5

Boafo-Arthur, S., & Brown, K. E. (2017). International students and academic misconduct: Personal, cultural, and situational variables. In *Handbook of research on academic misconduct in higher education* (pp. 286-305). IGI Global. https://doi.org/10.4018/978-1-5225-1610-1.ch013

Burgason, K. A., Sefiha, O., & Briggs, L. (2019). Cheating is in the eye of the beholder: An evolving understanding of academic misconduct. *Innovative Higher Education, 44*(3), 203-218. https://doi.org/10.1007/s10755-019-9457-3

Burke, M. M., & Bristor, J. (2017). Academic integrity policies: Has your institution implemented an effective policy? *The Accounting Educators' Journal, 46*(6), 928-942.

Bygrave, C., & Aşık, Ö. (2019). Global perspectives on academic integrity. In J. Hoffman, P. Blessinger, & M. Makhanya (Eds.), *Strategies for fostering inclusive classrooms in higher education: International perspectives on equity and inclusion* (pp. 19-33). Emerald Publishing. https://doi.org/10.1108/S2055-364120190000016003

Byun, J., Park, J., & Oh, A. (2020, August). Detecting contract cheaters in online programming classes with keystroke dynamics. In *Proceedings of the Seventh ACM Conference on Learning@ Scale* (pp. 273-276). https://doi.org/10.1145/3386527.3406726

Ćerimagić, S., & Hasan, M.R. (2019). Online exam vigilantes at Australian universities: Student academic fraudulence and the role of universities to counteract. *Universal Journal of Educational Research, 7,* 929-936. https://doi.org/10.13189/ujer.2019.070403

Chapman, D. W., & Lindner, S. (2016). Degrees of integrity: The threat of corruption in higher education. *Studies in Higher Education, 41*(2), 247-268. https://doi.org/10.1080/03075079.2014.927854

Chin, M. (2020, April 29). Exam anxiety: How remote test-proctoring is creeping people out. *The Verge*. https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81,* 42-51. https://doi.org/10.1016/j.chb.2017.12.001

Costley, J. (2019). Student perceptions of academic dishonesty at a cyber-university in South Korea. *Journal of Academic Ethics, 17*(2), 205-217. https://doi.org/10.1007/s10805-018-9318-1

Dalal, N. (2019). Exploring reflective means to handle plagiarism. *Journal of Information Systems Education, 27*(3), 175-184.

Daugherty, P. R., Wilson, H. J., & Chowdhury, R. (2019). Using artificial intelligence to promote diversity. *MIT Sloan Management Review, 60*(2), 1-5.

Denisova-Schmidt, E., Huber, M., & Leontyeva, E. (2016). On the development of students' attitudes towards corruption and cheating in Russian universities. *European Journal of Higher Education, 6*(2), 128-143. https://doi.org/10.1080/21568235.2016.1154477

Dow, G. T. (2015). Do cheaters never prosper? The impact of examples, expertise, and cognitive load on cryptomnesia and inadvertent self-plagiarism of creative tasks. *Creativity Research Journal, 27*(1), 47-57. https://doi.org/10.1080/10400419.2015.992679

Ferenbok, J., Mann, S., & Michael, K. (2016). The changing ethics of mediated looking: Wearables, veillances, and power. *IEEE Consumer Electronics Magazine, 5*(2), 94-102. https://doi.org/10.1109/MCE.2016.2516139

Florczak, I., & Wujczyk, M. (2020). The lie as a privacy protection measure. In *Performance appraisal in modern employment relations* (pp. 137-163). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-26538-0_7

Fort, T. L., Raymond, A. H., & Shackelford, S. J. (2016). Angel on your shoulder: Prompting employees to do the right thing through the use of wearables. *The Northwestern Journal of Technology & Intellectual Property, 14*, 139-179. https://doi.org/10.2139/ssrn.2661069

Gallant, T. B., Binkin, N., & Donohue, M. (2015). Students at risk for being reported for cheating. *Journal of Academic Ethics, 13*(3), 217-228. https://doi.org/10.1007/s10805-015-9235-5

Giattino, C. M., Kwong, L., Rafetto, C., & Farahany, N. A. (2019, January). The seductive allure of artificial intelligence-powered neurotechnology. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 397-402). https://doi.org/10.1145/3306618.3314269

Grym, J., & Liljander, V. (2016). To cheat or not to cheat? The effect of a moral reminder on cheating. *Nordic Journal of Business, 65*(3-4), 18-37.

Harding, J. M. (2018). *Performance, transparency, and the cultures of surveillance*. University of Michigan Press. https://doi.org/10.3998/mpub.9780711

Harwell, D. (2020, April 4). Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance. *Washington Post*. https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/

Heilweil, R. (2020, May 4). Paranoia about cheating is making online education terrible for everyone. *Vox*. https://www.vox.com/recode/2020/5/4/21241062/schools-cheating-proctorio-artificial-intelligence

Hoffmann, A. L. (2019). Where fairness fails: Data, algorithms, and the limits of antidiscrimination discourse. *Information, Communication & Society, 22*(7), 900-915. https://doi.org/10.1080/1369118X.2019.1573912

Högberg, R. (2011). Cheating as subversive and strategic resistance: Vocational students' resistance and conformity towards academic subjects in a Swedish upper secondary school. *Ethnography and Education, 6*(3), 341-355. https://doi.org/10.1080/17457823.2011.610584

Hong, J., & Baker, M. (2014). Wearable computing. *IEEE Pervasive Computing, 13*(2), 7-9. https://doi.org/10.1109/MPRV.2014.39

Hubler, S. (2020, May 10). Keeping online testing honest? Or an Orwellian overreach? *New York Times*. https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html

James, R. (2016). Tertiary student attitudes to invigilated, online summative examinations. *International Journal of Educational Technology in Higher Education, 13*(1), 19-32. https://doi.org/10.1186/s41239-016-0015-0

Introna, L. D. (2016). Algorithms, governance, and governmentality: On governing academic writing. *Science, Technology, & Human Values, 41*(1), 17-49. https://doi.org/10.1177/0162243915587360

Kaiser, R. B., & Hogan, R. (2010). How to (and how not to) assess the integrity of managers. *Consulting Psychology Journal: Practice and Research, 62*(4), 216-234. https://psycnet.apa.org/doi/10.1037/a0022265\

Kempf, A. (2016). Implications: Synthesis of findings, resistance, and alternatives. In *The pedagogy of standardized testing* (pp. 161-192). Palgrave Macmillan. https://doi.org/10.1057/9781137486653_8

Klein, M. (2020, June 13). CUNY professors uncover 'scandalous' level of cheating in final exams. *New York Post.* https://nypost.com/2020/06/13/cuny-professors-uncover-scandalous-level-of-cheating-in-final-exams/

Kolowich, S. (2013, April 15). Behind the webcam's watchful eye, online proctoring takes hold. *Chronicle of Higher Education.* https://www.chronicle.com/article/Behind-the-Webcams-Watchful/138505

Lingel, J., & Sinnreich, A. (2016). Incoded counter-conduct: What the incarcerated can teach us about resisting mass surveillance. *First Monday, 21*(5). https://doi.org/10.5210/fm.v21i5.6172

Lipson, S. M., & Karthikeyan, L. (2016). The art of cheating in the 21st Millennium: Innovative mechanisms and insidious ploys in academic deceit. *International Journal of Education, 8*(2), 48-72. https://doi.org/10.5296/ije.v8i2.9117

Liyanagunawardena, T. R., Adams, A. A., & Williams, S. A. (2013). MOOCs: A systematic study of the published literature 2008-2012. *The International Review of Research in Open and Distributed Learning, 14*(3), 202-227. https://doi.org/10.19173/irrodl.v14i3.1455

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review, 95*, 53-125.

Majeed, A., Baadel, S., & Haq, A. U. (2017, January). Global triumph or exploitation of security and privacy concerns in e-learning systems. In *International conference on global security, safety, and sustainability* (pp. 351-363). Springer. https://doi.org/10.1007/978-3-319-51064-4_28

Malesky Jr., L. A., Baley, J., & Crow, R. (2016). Academic dishonesty: Assessing the threat of cheating companies to online education. *College Teaching, 64*(4), 178-183. https://doi.org/10.1080/87567555.2015.1133558

Miller, A. D., Murdock, T. B., & Grotewiel, M. M. (2017). Addressing academic dishonesty among the highest achievers. *Theory into Practice, 56*(2), 121-128. https://doi.org/10.1080/00405841.2017.1283574

Moeck, P. G. (2002). Academic dishonesty: Cheating among community college students. *Community College Journal of Research and Practice, 26(*6), 479-491. https://doi.org/10.1080/02776770290041846

Moston, S., & Engelberg, T. (2019). And justice for all? How anti-doping responds to 'Innocent Mistakes.' *International Journal of Sport Policy and Politics, 11*(2), 261-274. https://doi.org/10.1080/19406940.2018.1550799

Muñoz, D. (2015, September 18). ProctorTrack Company releases statement on status of student data. *New Brunswick Today*. https://newbrunswicktoday.com/2015/09/18/proctortrack-company-releases-statement-on-status-of-student-data/

Muriel-Torrado, E., & Fernández-Molina, J. C. (2015). Creation and use of intellectual works in the academic environment: Students' knowledge about Copyright and Copyleft. *Journal of Academic Librarianship, 41*(4), 441-448. https://doi.org/10.1016/j.acalib.2015.05.001

Oravec, J. A. (2015). Gamification and multigamification in the workplace: Expanding the ludic dimensions of work and challenging the work/play dichotomy. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *9*(3). https://doi.org/10.5817/CP2015-3-6

Oravec, J. A. (2017). The manipulation of scholarly rating and measurement systems: Constructing excellence in an era of academic stardom. *Teaching in Higher Education*, *22*(4), 423-436. https://doi.org/10.1080/13562517.2017.1301909

Oravec, J. A. (2020). Online social shaming and the moralistic imagination: The emergence of Internet-based performative shaming. *Policy & Internet*, *12*(3), 290-310. https://doi.org/10.1002/poi3.226

Oravec, J. A. (2022). *Good Robot, Bad Robot: Dark and Creepy Sides of Robotics, Autonomous Vehicles, and AI*. Springer Nature.

OReilly, G., & Creagh, J. (2016, April). A categorization of online proctoring. In *Global learn* (pp. 542-552). Association for the Advancement of Computing in Education (AACE).

Owen, R. S. (2016). Cheating in online courses for financial aid fraud in the US. *Practice, 6*(2), 116-133. https://doi.org/10.5929/2016.6.2.7

Pan, M., Stiles, B. L., Tempelmeyer, T. C., & Wong, N. (2019). A cross-cultural exploration of academic dishonesty: Current challenges, preventive measures, and future directions. In *Prevention and detection of academic misconduct in higher education* (pp. 63-82). IGI Global. https://doi.org/10.4018/978-1-5225-7531-3.ch003

Pathak, B. K. (2016). Emerging online educational models and the transformation of traditional universities. *Electronic Markets, 26*(4), 315-321. https://doi.org/10.1007/s12525-016-0223-4

Perry-Hazan, L., & Birnhack, M. (2016). Privacy, CCTV, and school surveillance in the shadow of imagined law. *Law & Society Review, 50*(2), 415-449. https://doi.org/10.1111/lasr.12202

Roberts, L. A., & Todd, M. M. (2019). Let's be honest about law school cheating: A low-tech solution for a high-tech problem. *Akron Law Review, 52*(4), 1155-1189. https://ideaexchange.uakron.edu/akronlawreview/vol52/iss4/5

Rozario, A. (2020). FAQ: How was GMAT held using AI proctors? *The Quint*. https://www.thequint.com/news/education/what-is-an-artificial-intelligence-proctored-test-can-it-detect-cheating-faq

Semko, J. A., & Hunt, R. (2013). Legal matters in test security. In J. A. Wollack & J. J. Fremer (Eds.), *Handbook of test security* (pp. 237-255). Routledge.

Shams, S. M. R. (2017). International education management: Implications of relational perspectives and ethnographic insights to nurture international students' academic experience. *Journal for Multicultural Education, 11*(3), 206-223. https://doi.org/10.1108/JME-11-2015-0034

Singer, N. (2015, April 6). Online test-takers feel software's uneasy glare. *The New York Times*. Section B, 1. https://www.nytimes.com/2015/04/06/technology/online-test-takers-feel-anti-cheating-softwares-uneasy-glare.html

Slade, C., Rowland, S., & McGrath, D. (2019). Talking about contract cheating: Facilitating a forum for collaborative development of assessment practices to combat student dishonesty. International *Journal for Academic Development, 24(*1), 21-34. https://doi.org/10.1080/1360144X.2018.1521813

Song-Turner, H. (2008). Plagiarism: Academic dishonesty or 'blind spot' of multicultural education? *Australian Universities' Review, 50*(2), 39-50.

Sprague, R. (2015). Welcome to the machine: Privacy and workplace implications of predictive analytics. *Richmond Journal of Law & Technology, 21*(4), 1-46. http://dx.doi.org/10.2139/ssrn.2454818

Stoesz, B. M., Eaton, S. E., Miron, J., & Thacker, E. J. (2019). Academic integrity and contract cheating policy analysis of colleges in Ontario, Canada. *International Journal for Educational Integrity, 15*(4). https://doi.org/10.1007/s40979-019-0042-4

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

Taylor, E. (2013). *Surveillance schools: Security, discipline and control in contemporary education.* Springer. https://doi.org/10.1057/9781137308863

Tene, O., & Polonetsky, J. (2013). Judged by the tin man: Individual rights in the age of big data. *Journal on Telecommunications & High Technology Law, 11*, 351-369.

Tomlinson, M. (2016). The impact of market-driven higher education on student-university relations: Investing, consuming and competing. *Higher Education Policy, 29*(2), 149-166. https://doi.org/10.1057/hep.2015.17

Tonguç, G., & Ozkara, B. O. (2020). Automatic recognition of student emotions from facial expressions during a lecture. *Computers & Education*, *148*. https://doi.org/10.1016/j.compedu.2019.103797

Traoré, I., Nakkabi, Y., Saad, S., Sayed, B., Ardigo, J.D., & de Faria Quinan, P.M. (2017). Ensuring online exam integrity through continuous biometric authentication. In *Information Security Practices* (pp. 73-81). Springer International Publishing. https://doi.org/10.1007/978-3-319-48947-6_6

Turner, C. (2016, October 11). Boarding school principal 'gave go ahead on exam cheating.' *The Daily Telegraph*, 11. https://www.telegraph.co.uk/education/2016/10/10/boarding-school-principal-gave-go-ahead-on-exam-cheating/

Underwood, R.H. (1995). Truth verifiers: From the hot iron to the lie detector. *Kentucky Law Journal, 84,* 597-642.

Vanacker, B. (2011). Returning students' right to access, choice and notice: A proposed code of ethics for instructors using Turnitin. *Ethics and Information Technology, 13*(4), 327-338. https://doi.org/10.1007/s10676-011-9277-3

Vegendla, A., & Sindre, G. (2019). Mitigation of cheating in online exams: Strengths and limitations of biometric authentication. In *Biometric authentication in online learning environments* (pp. 47-68). IGI Global. https://doi.org/10.4018/978-1-5225-7724-9.ch003

Verplaetse, J., Vanneste, S. & Braeckman, J. (2007). You can judge a book by its cover: The sequel: A kernel of truth in predictive cheating detection. *Evolution and Human Behavior, 28*(4), 260-271. https://doi.org/10.1016/j.evolhumbehav.2007.04.006

Weidman, J., & Grossklags, J. (2018). *What's in your policy? An analysis of the current state of information security policies in academic institutions.* Aisel Research Paper #23. https://aisel.aisnet.org/ecis2018_rp/23/

Wright, E. (2018). The future of facial recognition is not fully known: Developing privacy and security regulatory mechanisms for facial recognition in the retail sector. *Fordham Intellectual Property, Media, & Entertainment Law Journal, 29*, 611-642.

Yorke, J., Sefcik, L., & Veeran-Colton, T. (2020, forthcoming). Contract cheating and blackmail: a risky business? *Studies in Higher Education*, 1-14. https://doi.org/10.1080/03075079.2020.1730313

Zamastil, K. (2004). Legal issues in US higher education. *Common Law Review, 6,* 70-94.

Zeng, Y., Lu, E., Sun, Y., & Tian, R. (2019). *Responsible facial recognition and beyond.[* preprint]. arXiv:1909.12935.

Zhang, Y. H. (2016). What is plagiarism? In *Against plagiarism* (pp. 3-12). Springer International Publishing. https://doi.org/10.1007/978-3-319-24160-9

About the Author

Jo Ann Oravec
University of Wisconsin-Whitewater, University of Wisconsin-Madison
oravecj@uww.edu
https://orcid.org/0000-0003-1716-7969
Jo Ann Oravec, PhD, MBA, MS, MA, is a professor of information technology and supply chain management at the University of Wisconsin at Whitewater. She is also affiliated with the Holtz Center for Science and Technology Studies at the University of Wisconsin at Madison.

education policy analysis archives

Volume 30 Number 175 December 6, 2022 ISSN 1068-2341