You must have your webcam on for the entire duration of the examination: the trade-off between the integrity of on-line assessments and the privacy rights of students

Damian Gordon, John Paul Gibson, Brendan Tierney, Dympna O'Sullivan, Ioannis Stavrakakis

"YOU MUST HAVE YOUR WEBCAM ON FOR THE ENTIRE DURATION OF THE EXAMINATION": THE TRADE-OFF BETWEEN THE INTEGRITY OF ON-LINE ASSESSMENTS AND THE PRIVACY RIGHTS OF STUDENTS

Damian Gordon, J. Paul Gibson, Brendan Tierney, Dympna O'Sullivan, Ioannis Stavrakakis

Technological University of Dublin (Ireland), Institut Mines-Télécom (France), Technological University of Dublin (Ireland), Technological University of Dublin (Ireland), Technological University of Dublin (Ireland)

Damian.X.Gordon@TUDublin.ie; Paul.Gibson@Telecom-SudParis.eu; Brendan.Tierney@TUDublin.ie; Dympna.OSullivan@TUDublin.ie; Ioannis.Stavrakakis@TUDublin.ie

ABSTRACT

The impact of COVID-19 has been widespread and far-reaching, and one domain that has experienced severe disruption is the university education sector, where the entire apparatus of teaching and assessment for many programmes of study had to move on-line in a matter of days[10]. This was accomplished notably through enormous co-operation between staff and students in educational institutions (Adnan and Anwar, 2020). The negative economic impacts of COVID-19 on university students has been highlighted in terms of poor access to online resources, delayed graduation and lost internships with this effect felt more keenly by students from low socioeconomic backgrounds (Aucejo, et al. 2020). However, an issue that has been less reported is how the crisis highlighted mismatches between on the one hand the regulations and requirements of the educational institutions, and on the other hand the privacy rights (and needs) of the students.

In this research we are investigating the challenges associated with the potential for students and teachers to inadvertently share aspects of their private lives as part of on-line teaching and assessment, as well as the ethical challenges of monitoring students during exams. Some educational institutes have used software for monitoring students during assessments (called *e-Proctoring systems* (González-González, et al., 2020)), and these systems lead to a range of potential ethical concerns, particularly if the systems employ facial detection (or recognition) systems and/or artificial intelligence systems to detect potential malfeasance.

One voice that hasn't been included in this discussion heretofore is the student voice, so this research includes the design and development of the *WebCam Usage Student Survey* (*WUSS*), and a group of computer science students (N=44) were asked for their opinions on a wide range of privacy issues (as these students have some idea on the potential pitfalls of using these types of technologies). Their views are varied and nuanced, and their perspective in combination with the literature provide a complex picture of the ethics of online interactions.

This issue is one of a rapidly growing number of computer ethics issues that have been emerging recently, to such an extent that a number of third-level institutes across Europe are collaborating to explore some of these key ethical challenges, and to develop educational content that is both based

[10] https://www.timeshighereducation.com/hub/keystone-academic-solutions/p/impact-coronavirus-higher-education

on pedagogically sound principles, and motivated by international exemplars of best practice to highlight these matters as part of the Erasmus+ Ethics4EU project[11] (O'Sullivan and Gordon, 2020).

INTRODUCTION

Given the abrupt nature of the move to on-line teaching that was dictated by COVID-19, educational institutions were not necessarily in a position to fully consider the ethical ramifications of their decisions, or to update their policy documents. Many were also unable to obtain so-called "wet signatures" for explicit consent forms from students for this new approach, or for the use of e-Proctoring systems (González-González, et al., 2020). Student groups and Digital Rights advocates have begun to raise significant concerns about these systems, and the mandatory use of webcams in on-line teaching and assessment. A news article by Nir Kshetri in "The Conversation" on November 6th, 2020[12] points out that in America organisations such as the Electronic Frontier Foundation have filed numerous petitions to academic institutes and legislative bodies to call for educational administrators and teachers to end the use of these systems, and categorised their use as "spying".

Some have argued that the best way to deal with these issues is to avoid them altogether, so to have neither students nor teachers to ever turn on their webcams during lessons, and to change the type of assessment to one that doesn't require invigilation, for example, using open-book examinations which are mainly focused on applying knowledge as opposed to assessing basic recall (Remtulla, 2020). In situations where this is possible, it is a viable approach, although since the introduction of the Bologna process in 1999 (which impacted higher education in 29 European countries), with its emphasis on learning outcomes, it is more challenging to develop more open and individualised assessment approaches (Murtonen, et al., 2017; Zeide and Nissenbaum, 2018).

If students and teachers are required to share their webcams, this may inadvertently lead to them sharing aspects of their private lives as part of on-line teaching and assessment, this could include sharing visual information about their private residences; or sharing audio information that might reveal too much information about their private lives. On the other hand, some teachers feel it is difficult to foster a connection with their students without seeing their faces, and encourage students to share their webcams, this can sometimes unintentionally cause students to feel anxious (a particular concern for students appears to be concern over their peers' perceptions of them (Rajab and Soheib, 2021). Further issues might arise if the staff or students are *required* by their educational institute to always have their webcams on during lessons or assessments. This can blur the differentiation between public spaces and private spaces, which philosophers like Jürgen Habermas (1991) and Hannah Arendt (1998) have explored through questions of ownership and property, and they asked questions such as; "Who owns resources in these spaces?" and "What is truly private?" There are also a number of other "divides" worth exploring: race, social status, gender, etc. For example, in the context of gender, female students and staff tend to be more cautious about sharing their webcams, as they are more likely to be harassed and exposed to aggressive behaviours in an on-line setting (Chawki and el Shazly, 2013).

Educational institutions that require students to use webcams to be active during online assessments often use software called e-Proctoring systems to monitor the activities of the students during the assessment process. These systems replace a human invigilator (or *proctor*) who ensures that all of the necessary examination regulations are adhered to, and help to prevent cheating in a brick-and-mortar

[11] http://ethics4eu.eu/

[12] https://theconversation.com/remote-education-is-rife-with-threats-to-student-privacy-148955

educational setting. There are a growing number of such systems available, such as Remote Proctor NOW (RPNOW), eProctoring, SMOWL and ProctorExams (González-González, et al., 2020), and these e-Proctoring systems typically can be either manual or automated, where manual proctoring (also known as *Live Proctoring*) is remote invigilation where a person is actively supervising the test-taker throughout the assessment, whereas automated proctoring uses technologies such as machine learning and facial detection to monitor both the test-taker and their technologies, including laptops, tablets, and mobile phones. These systems raise a number of security and fairness considerations (Langenfeld, 2020), additionally at least one of these systems have trouble detecting persons-of-colour[13]. It is worth noting that students do not always have full control over the environment in which they take their examinations, whether in student residences or in a family home, if someone enters the room that they are in, or a noise is heard in the background, some of the automated systems will log the student out, and others will even summarily fail them. Some e-Proctoring systems enforced these automated processes and others do not, so it is important that students and teachers be fully aware of the conditions and consequences of using these systems rather than allowing potential misinformation about the functions of these systems to increase their anxiety. In fact, De Santis, et al. (2020) found that students who have used e-Proctoring systems previously (whether automated or manual) are significantly more confident with their use for assessment purposes.

Some of the issues around student anxiety appear to originate from concerns around surveillance, and from a philosophical perspective such systems cannot fail but bring to mind the notion of a *Panopticon*, a building design (and a system of control) that allows all people in that building to be observed by a single, central observer. Developed by English philosopher and social theorist Jeremy Bentham in the 18th century, the concept has been viewed as the blueprint for a tool of oppression and social control by philosophers like Michel Foucault (1977) and Gilles Deleuze (1992), who see such systems as a means of control by groups of people (including students) through disciplinary power. Allen (2012), Tufekci (2017), Zuboff (2019) and Vatcha (2020) further explore the nature of digital surveillance, and such considerations should be incorporated into the decision-making processes of educational institutes when they are considering the use of e-Proctoring systems.

Another area of concern is that a minority of these systems require that students display some form of identification (e.g. passport or driving license) to validate the initial system login process, this represents a significant security concern, as it is possible in some of these systems for third-parties to intercept the video and audio information being transmitted (notably, intruders have been able to gain access to Zoom classrooms - known as "Zoombombing" - due to issues with Zoom's cybersecurity). This leads to a range of serious questions about the recording and retention of this data, and particularly around the issue of ownership of that data. Even if it were possible to establish legally by whom the data is owned (potentially the students, the platform suppliers, the educational institution, or some combination of these stakeholders), the ethical ownership of this data is far less clear. A concomitant consideration is around the issue of consent; how can it be given if the ownership of the data is difficult to establish, and how can it be meaningful if it isn't clear how this data will be used in the future? In general, the use of automated machine learning and facial detection techniques in any computer system should be viewed as a matter of concern, especially since on 30th June 2020, the Association for Computing Machinery (the professional body for computer professionals) called for the cessation of all use of facial recognition technologies, as they produce "*results demonstrating clear bias based on ethnic, racial, gender, and other human characteristics recognizable by computer systems*" (ACM, 2020). Andrejevic and Selwyn (2020) examined the issue of facial recognition in the

[13] https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning

educational context, and raised concerns around the dehumanising nature of this technology, which can lead to the foregrounding of gender and race, as well as concerns around the dangers of using the data from these systems in automated decision support systems.

Researchers S.E. Eaton and K.L. Turner (2020) highlight concerns about the relationship between e-Proctoring systems and student mental health, and conclude that more research needs to be done to explore their relationship. Regehr and McCahan (2020) note that e-Proctoring systems have been used to an unprecedented level during the COVID-19 crisis, which has resulted in a number of scalability and technical challenges, including connectivity issues for students, which has contributed significantly to their stress levels, and opens up the possibility of sharing exam questions between students taking the same examination at different times. Coghlan, et al. (2020) philosophically analyse e-Proctoring systems, and they highlight some of the dangers of these systems, such as in one case when a student's credit card details were accidentally displayed on their computer screen. They conclude that educational institutes must be accountable when mistakes occur, but that the students also bear some responsibility for their choices.

METHODS

An important element that seems to be missing from much of the research heretofore is the inclusion of students' voices in the analysis, therefore this research was designed to incorporate their contributions to this debate. To achieve this, a new survey instrument, the *WebCam Usage Student Survey* (*WUSS*), was developed, inspired by a number of questionnaires related to on-line privacy, and particularly the *Privacy Attitudes Questionnaire* (PAQ) by Chignell, et al. (2003), as that instrument most closely aligns to the goals of this research. It has a number of Likert scales (from *Strongly Disagree* to *Strongly Agree*) that relate to different categories of privacy, and for this research we took the nine questions from the PAQ that relate to the category of *Willingness to be Monitored*, as a springboard for the development of our instrument. Those questions were:

1. I frequently would like to block my phone number on call display
2. I respond to telephone marketing surveys
3. I prefer not to have my name listed on a building directory
4. I would give my home phone number to business clients
5. I like to fill out surveys and contests
6. Red light (intersection) cameras should be used
7. Speeding cameras should be used
8. Insurance companies should not have access to people's health records
9. CCTV should be used in public places to improve public safety and security

However, Question 4 was changed from "business clients" to "lecturers" to make it more applicable to students. Following this, a number of questions were developed and trialled to look more specifically at issues related to webcam usage, and ultimately seven more questions were added to the questionnaire using the same structure and phraseology as the PAQ, as follows:

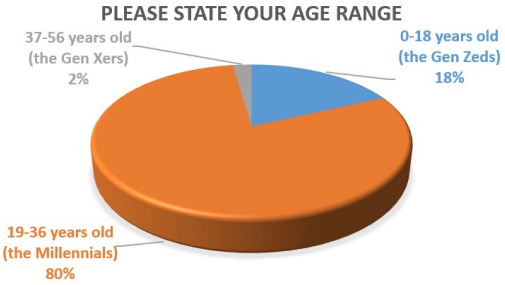
1. I use privacy software or incognito browsing to protect my privacy online
2. I have used the (sliding) camera cover to block the webcam, or have blocked the camera in some other way.
3. It should be mandatory for students to have their webcams on during class
4. It should be mandatory for students to have their webcams on during exams
5. Facial recognition software should be used with the students' webcams to ensure the right person is doing the exam
6. Artificial Intelligence systems should be used with the students' webcams to log the student out of the exam if the system thinks they are doing something suspicious
7. I treat the webcams on my laptop, tablet, and mobile phone in the same way, in terms of privacy considerations

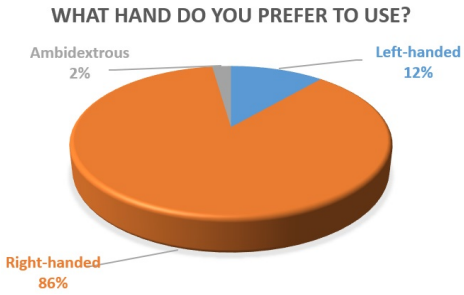
Additionally, demographics questions were added to explore if there are any disparities in the perspectives of different groups of students, based on surveys by Kezer, et al. (2016) and Umawang (2019). The additional questions enquired the students age ranges, handedness, gender, county of origin, primary language, and whether they wear corrective lenses. These are as follows:

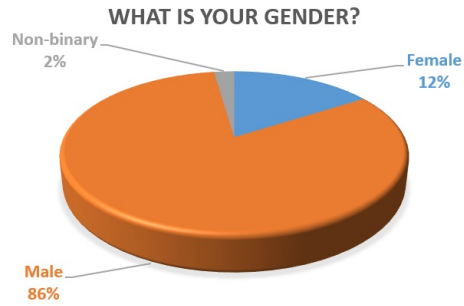
1. Please choose your age range
2. Do you wear corrective lenses (glasses, contact lenses, etc.)?
3. What hand do you prefer to use?
4. Is English your first language?
5. Country of origin (optional)
6. What is your gender?

The survey was given to a range of students enrolled in computer science programmes (both undergraduate and postgraduate). Because the students already have some understanding of both the benefits and pitfalls of the technologies associated with this scenario (for example, Artificial Intelligence, Machine Learning, Image Processing, and Computer Vision), it was felt that they would be able to offer an informed opinion on these matters. It was created using Microsoft Forms, and was distributed from April 21st to April 26th, 2021. The students were given the following key instructions: that the survey is voluntary, that all submissions do not record the students' names, and that the results will be published as part of the broader discussion on these issues. A total of 44 students participated in the survey, and Table 1 presents the demographic results of those participants.

Table 1. Responses to Demographic Questions.







Countries of Origin:

Ireland: 22 participants

Philippines: 4 participants

China: 2 participants

India: 2 participants

Poland: 2 participants

England: 1 participant

Malaysia: 1 participant

Malta: 1 participant

Romania: 1 participant

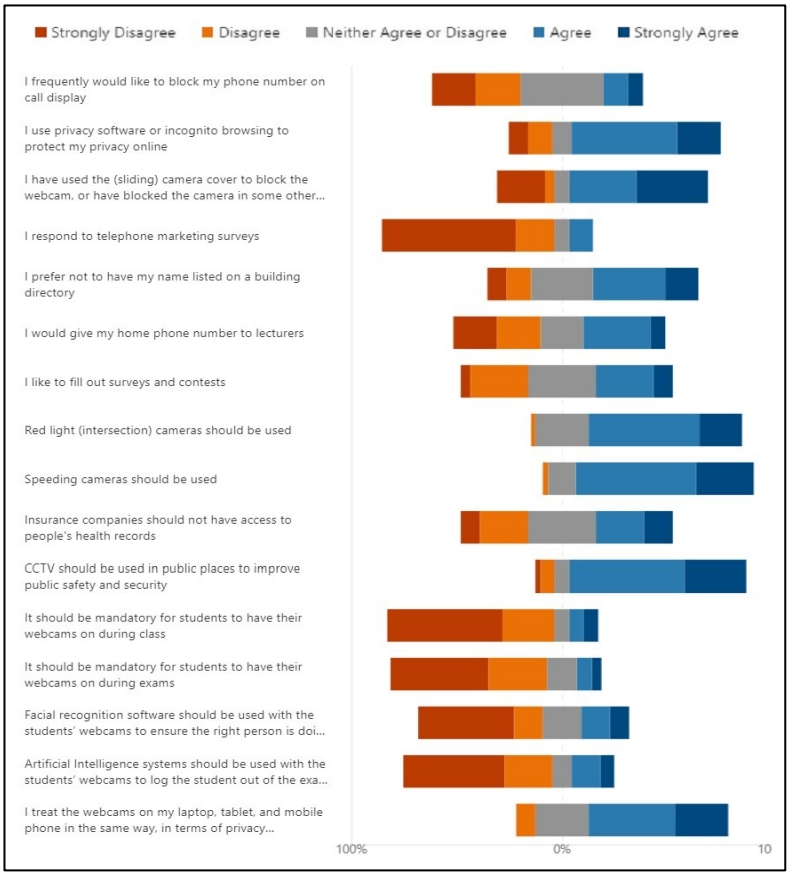
Syria: 1 participant

Vietnam: 1 participant

As would be expected from Computer Science studentgroups, the majority of respondents are male, and principally millennials (in the age range 19-36 years old). There is a reasonable distribution of those who wear corrective lenses, and those who don't, as well as those for whom English is their first language, and those it isn't. The participants represent students from 11 countries, with the majority from Ireland (the country where the survey was conducted).

Following these questions, the rest of the survey was concerned with presenting the privacy scenarios developed from the combination of the PAQ questionnaire and the questions added for this research. Table 2 presents the results of those questions.

Table 2. Responses to Privacy Scenarios.



There are several noteworthy outcomes from this portion of the survey, but the most important overriding message is that there is no scenario that the students are completely unanimous about; although there are some scenarios that the majority of students show some agreement on.

Scenarios where the majority of students either *Agreed* or *Strongly Agreed*, include "*I use privacy software or incognito browsing to protect my privacy online*" at a rate of 70.5%, "*I have used the (sliding) camera cover to block the webcam, or have blocked the camera in some other way*" at 65.9%, and "*I treat the webcams on my laptop, tablet, and mobile phone in the same way, in terms of privacy considerations*" also at 65.9%. These three results combined would tend to suggest that students are generally concerned about their privacy in their private spaces. And these are further supported by the following answers that students also either *Disagreed* or *Strongly Disagreed* with "*It should be mandatory for students to have their webcams on during class*" (79.5%), "*It should be mandatory for students to have their webcams on during exams*" (74.4%), "*Facial recognition software should be used with the students' webcams to ensure the right person is doing the exam*" (59.1), and "*Artificial Intelligence systems should be used with the students' webcams to log the student out of the exam if the system thinks they are doing something suspicious*" (70.4%).

In contrast to their views on private spaces, the students were far less concerned about their privacy in public spaces, for example, "*Red light (intersection) cameras should be used*" (students either *Agreed* or *Strongly Agreed* at a rate of 72.7%), "*Speeding cameras should be used*" (84.1%), and "*CCTV should be used in public places to improve public safety and security*" (84%). These three results combined would tend to suggest that students are generally less concerned about their privacy in public spaces.

It is worth noting that there was no significant difference found in responses between different demographic groups amongst the participants, but this may be due to the sample size, as was noted already, the majority of respondents were male and in the millennial age range. It is also worth noting that research has consistently shown that millennials are confused on the topic of privacy, for example, a study by the USC Annenberg Center for the Digital Future and Bovitz Inc.[14] showed that although a majority of respondents agreed no one should have access to their data or online behaviour, 25% of them said they would exchange information for relevant advertising, 56% would share their location for coupons or deals, and 51% said they would share information with companies if they get something in return.

DISCUSSION

The purpose of this study is to explore ethical issues around the use of webcams and e-Proctoring systems, but not to portray these systems as being inherently problematic, nor is it intended to criticise the developers of these systems. At a time of global pandemic, it became necessary to change how teaching and assessment occurred, and educational institutions have been doing their best to fulfil their obligations to their students. Educators have been finding new ways to teach in these changed circumstances, and ways of connecting with their students, and even finding ways of leveraging the changes to help the teaching and learning process (for example, Jia, et al. (2020) used a variation of the flipped classroom model to improve student engagement). Crucially, these systems must be easy-to-use, and give control to the participants over what they choose to share. As mentioned previously, as well as privacy concerns, students have major concerns about judgement by their peers (Rajab and Soheib, 2021), so the systems must (both technically and procedurally) allow students to maintain the level of privacy that they desire. The outcomes of the *WebCam Usage Student Survey* (*WUSS*) address issues related to WebCam usage in general, as well as particularly in the case of e-Proctoring systems. The students' perspectives were varied and nuanced, and may indicate that the students are aware of the challenges of delivering educational content, and have been willing to forego aspects of their privacy for the sake of continuing their educational journey.

In the case of e-Proctoring systems, the key concerns relate to the potential lack of human agency in these systems, for example, if the systems are logging students out of an examination because of extraneous visual or audio inputs. However, it is worth noting that many of these systems do not take independent action, but rather notify a human proctor of suspected malfeasance, and the human must decide whether or not to take action. In fact, many of the concerns around these systems are as a result of the fact that they had to be rushed into service for such a wide variety of assessment processes in such a short period of time. As mentioned previously De Santis, et al. (2020) found that students who are knowledgeable about e-Proctoring systems are significantly more confident with their use in assessment, therefore it may the case that student anxiety about the use of these systems could abate if they are given more training on these systems, and more training on how they work. Additionally, it is important that teachers fully understand how these systems work so that they can instill confidence in their students.

It is hoped that discussions like these can serve as a reminder that all participants in the educational process have both rights and responsibilities in terms of their own privacy, and the privacy of others.

[14] https://www.forbes.com/sites/dianemehta/2013/04/26/new-survey-suggests-millennials-have-no-idea-what-privacy-means/?sh=20666b3229e2

CONCLUSIONS

This paper outlines an exploration of issues related to the use of webcams in an educational context, focusing in particular on some of the ethical considerations that have been exacerbated by the COVID-19 global pandemic. A review of some key literature is presented, focusing on some of those key ethical concerns, as well as presenting state-of-the-art research on the use of webcams since the onset of COVID-19. Following this the development of a survey to begin to capture the student voice in this discussion is presented, and the results of that survey are presented. The key outcome of the survey is that different students have different perspectives on these issues, so we are not seeing simplistic, binary, polarised thinking from students; the students who are most aware of the technological pitfalls of these systems, computer science students, understand that this is a nuanced issue with boons and banes, and therefore, to help educational organisations and individuals understand some of the challenges associated with the use of both WebCams and e-Proctoring systems, a discussion has presented, based on this work. The next step in this research is to create two sets of guidelines, one on webcam usage, and one on guidelines for e-Proctoring systems.

ACKNOWLEDGEMENTS

The authors of this paper and the participants of the Ethics4EU project gratefully acknowledge the support of the Erasmus+ programme of the European Union. The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. The authors also acknowledge the invaluable pedagogical and technological advice provided by Dr. Ciaran O'Leary (Technological University of Dublin) in the preparation of this publication.

KEYWORDS: Digital Ethics, Privacy, e-Proctoring, Webcams.

REFERENCES

ACM, 2020, Association for Computing Machinery, *Statement On Principles And Prerequisites For The Development, Evaluation And Use Of Unbiased Facial Recognition Technologies*, Available at: https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf

Adnan, M. and Anwar, K. (2020) "Online Learning amid the COVID-19 Pandemic: Students' Perspectives" *Journal of Pedagogical Sociology and Psychology*, 2(1), pp.45-51.

Allen, A.L., 2012. "What must we Hide: The Ethics of Privacy and the Ethos of Disclosure", *Thomas L. Rev.*, 25, p.1.

Andrejevic, M. and Selwyn, N. (2020) "Facial Recognition Technology in Schools: Critical Questions and Concerns", *Learning, Media and Technology*, 45(2), pp.115-128.

Arendt, Hannah (1998) "The Public and the Private Realm" In *The Human Condition*, pp. 182–230. Chicago, IL: University Of Chicago Press.

Aucejo, E.M., French, J., Araya, M.P.U. and Zafar, B. (2020) "The Impact of COVID-19 on Student Experiences and Expectations: Evidence from a Survey", *Journal of Public Economics*, 191, p.104271.

Chawki, M. and el Shazly, Y. (2013) “Online Sexual Harassment: Issues and Solutions”, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 4, p.71.

Chignell, M.H., Quan-Haase, A. and Gwizdka, J. (2003) The Privacy Attitudes Questionnaire (PAQ): Initial Development and Validation, In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 47, No. 11, pp. 1326-1330). Sage CA: Los Angeles, CA: SAGE Publications.

Coghlan, S., Miller, T. and Paterson, J. (2020) “Good Proctor or "Big Brother"? AI Ethics and Online Exam Supervision Technologies”. *arXiv preprint arXiv:2011.07647*.

Deleuze, Gilles (1992) “Postscript on the Societies of Control”, *October*, Vol. 59, pp. 3-7.

De Santis, A., Bellini, C., Sannicandro, K., Minerva, T. (2020) “Students’ Perception on E-Proctoring System for Online Assessment” In *EDEN 2020 Conference Proceedings*, No. 1, pp. 161-168.

Eaton, S.E. and Turner, K.L. (2020) “Exploring Academic Integrity and Mental Health during COVID-19: Rapid Review”, *Journal of Contemporary Education, Theory & Research*, 4(2), pp.35-41.

Foucault, Michel (1977) “Discipline and Punish: the Birth of the Prison”, New York: Random House.

González-González, C.S., Infante-Moro, A. and Infante-Moro, J.C. (2020) “Implementation of E-proctoring in Online Teaching: A Study About Motivational Factors”. *Sustainability*, 12(8), p.3488.

Habermas, Jürgen (1991) *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, MA: The MIT Press.

Jia, C., Hew, K. F., Bai, S., & Huang, W. (2020). “Adaptation of a Conventional Flipped Course to an Online Flipped Format during the COVID-19 Pandemic: Student Learning Performance and Engagement”, *Journal of Research on Technology in Education*, 1-21.

Kezer, M., Sevi, B., Cemalcilar, Z., Baruh, L. (2016) “Age differences in privacy attitudes, literacy and privacy management on Facebook”, *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(1).

Kshetri, N. (2020) “Remote education is rife with threats to student privacy”, The Conversation, November 6th, 2020. Full Content Available at: https://theconversation.com/remote-education-is-rife-with-threats-to-student-privacy-148955

Langenfeld, T. (2020) "Internet-Based Proctored Assessment: Security and Fairness Issues", *Educational Measurement: Issues and Practice*, 39(3), pp. 24-27.

Murtonen, M., Gruber, H. and Lehtinen, E. (2017) “The Return of Behaviourist Epistemology: A Review of Learning Outcomes Studies”, *Educational Research Review*, 22, pp.114-128.

O’Sullivan, D., Gordon, D. (2020) “Check Your Tech – Considering the Provenance of Data Used to Build Digital Products and Services: Case Studies and an Ethical CheckSheet”, IFIP WG 9.4 European Conference on the Social Implications of Computers in Developing Countries, 10th–11th June 2020, Salford, UK.

Rajab, M. H., Soheib, M. (2021) “Privacy Concerns Over the Use of Webcams in Online Medical Education During the COVID-19 Pandemic”, *Cureus*, 13(2).

Regehr, C. and McCahan, S. (2020) “Maintaining Academic Continuity in the Midst of COVID-19”, *Journal of Business Continuity & Emergency Planning*, 14(2), pp.110-121.

Remtulla, R. (2020) “The Present and Future Applications of Technology in Adapting Medical Education amidst the COVID-19 Pandemic”, *JMIR Medical Education*, 6(2), p.e20190.

Tufekci, Z. (2017) *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.

Umawang, J. (2019) "Labs Survey Finds Privacy Concerns, Distrust of Social Media Rampant with all Age Groups", Date Accessed: 10/5/2021, Full Content Available at: https://blog.malwarebytes.com/security-world/2019/03/labs-survey-finds-privacy-concerns-distrust-of-social-media-rampantwith-all-age-groups/

Vatcha, A. (2020) "Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees" *iSCHANNEL*, p.4.

Zeide, E. and Nissenbaum, H. (2018) "Learner Privacy in MOOCs and Virtual Education". *Theory and Research in Education*, 16(3), pp.280-307.

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books.