Plagiarism Detection Systems and Privacy: Balancing Academic Integrity and User Data Protection

Name:

Institution:

Chapter 4 – Results and Discussion

Introduction

The previous chapter has discussed how the secondary data for this research was collected and analyzed. This chapter will present the main results and a discussion of the results based on previous research. The chapter will include five main sections. These sections directly relate to the four research questions that were earlier mentioned as well as a separate discussion section for the findings. As mentioned in the methodology chapter, the online proctoring tools that will be studied in this research include Respondus, Proctorio, ProctorU, and Examity.

How Lockdown Browsers Operate

In order to understand how the online proctoring tools work, the four lockdown browsers were downloaded and installed in a controlled testing environment as illustrated in the figures below. The environment replicated the condition in which students typically use these browsers when taking online exams, ensuring that the analysis was carried out in a controlled and standardized setting. The figures illustrate the necessary steps for downloading and installing lockdown browsers with a specific focus on Respondus. The seventh step has been left out because it is usually specific to each institution of higher learning.

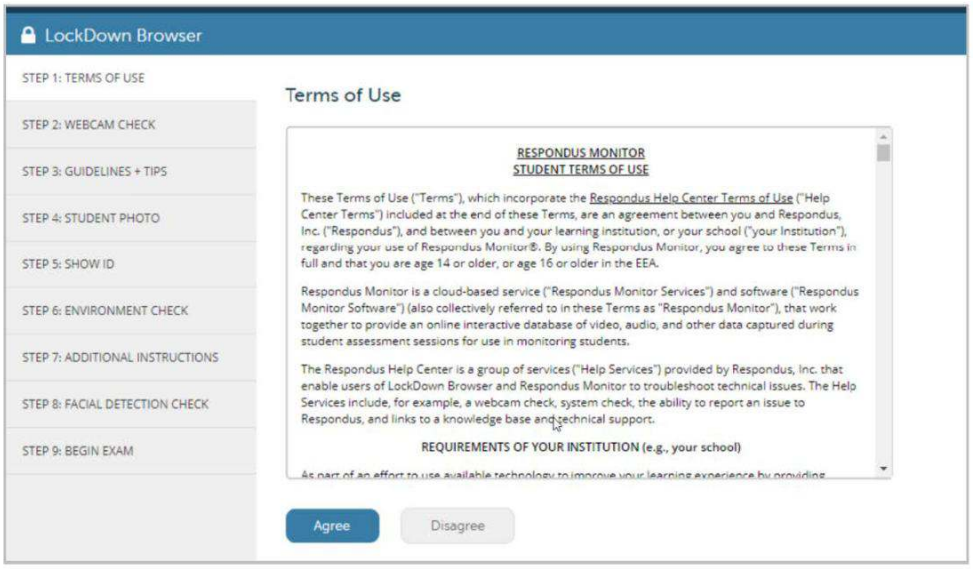

Figure 1: Step 1 of Installing Respondus Lockdown Browser

Figure 2: Step 2 of Installing Respondus Lockdown Browser

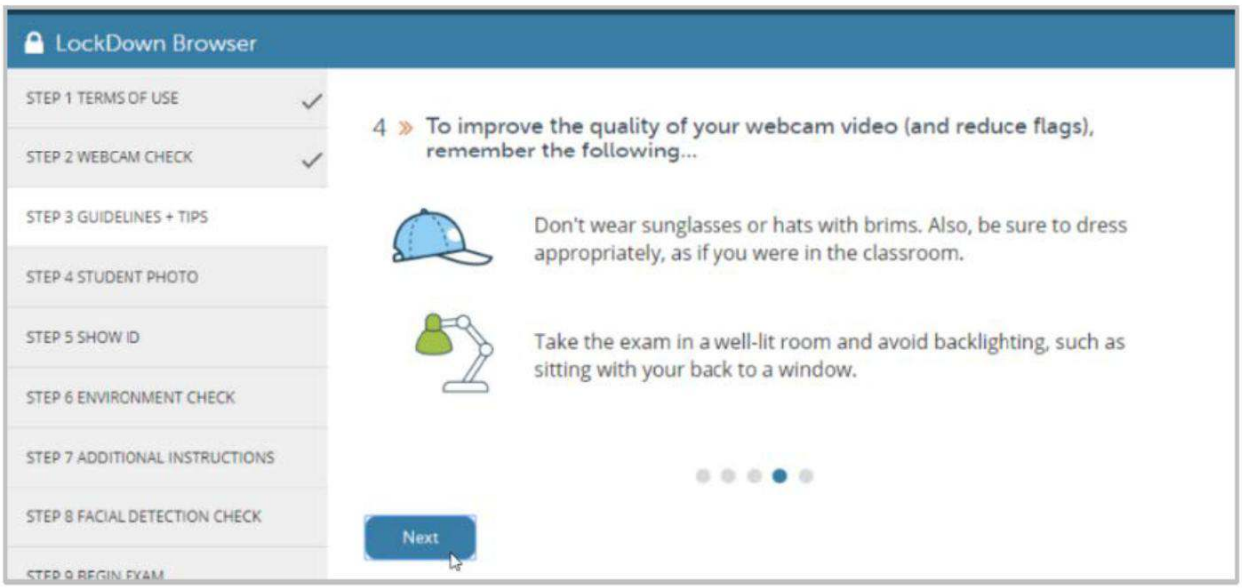

Figure 3: Step 3 of Installing Respondus Lockdown Browser

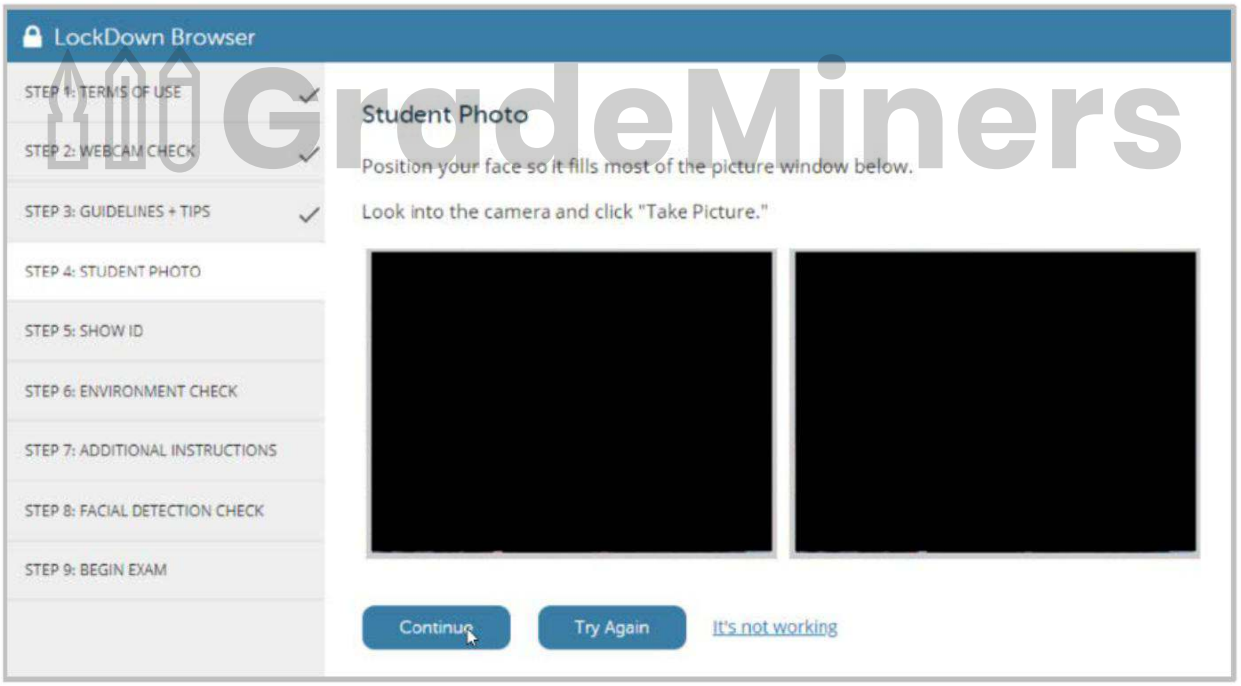

Figure 4: Step 4 of Installing Respondus Lockdown Browser

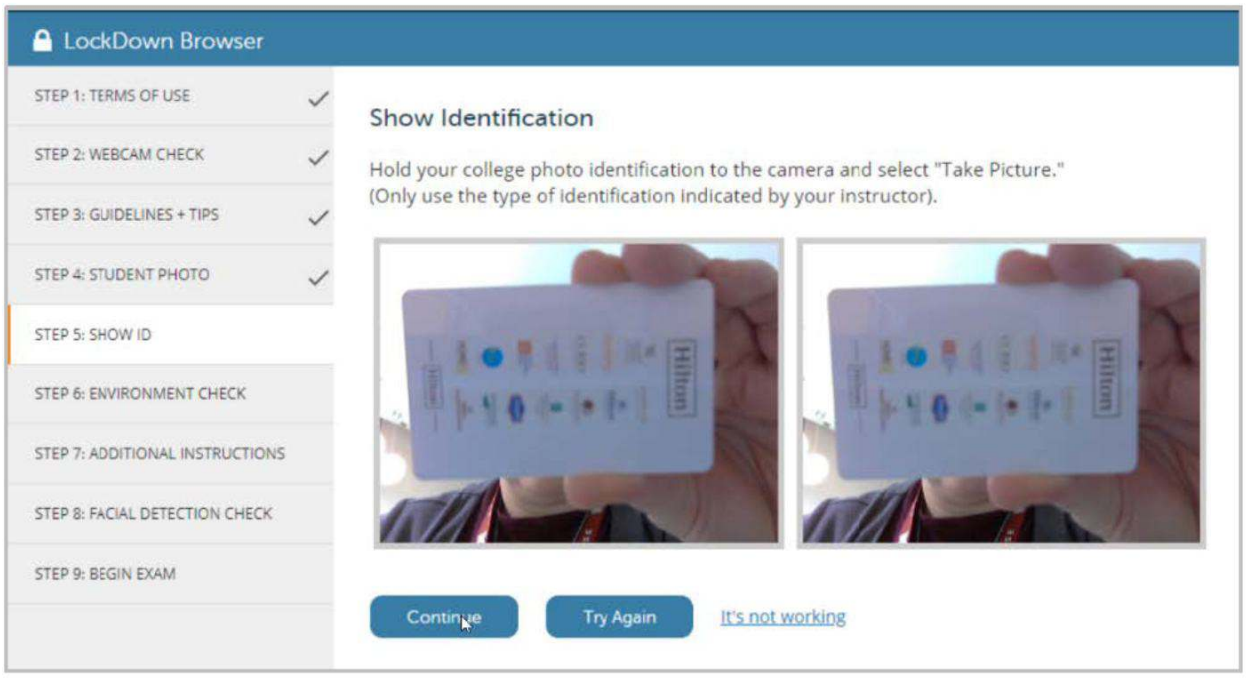

Figure 5: Step 5 of Installing Respondus Lockdown Browser

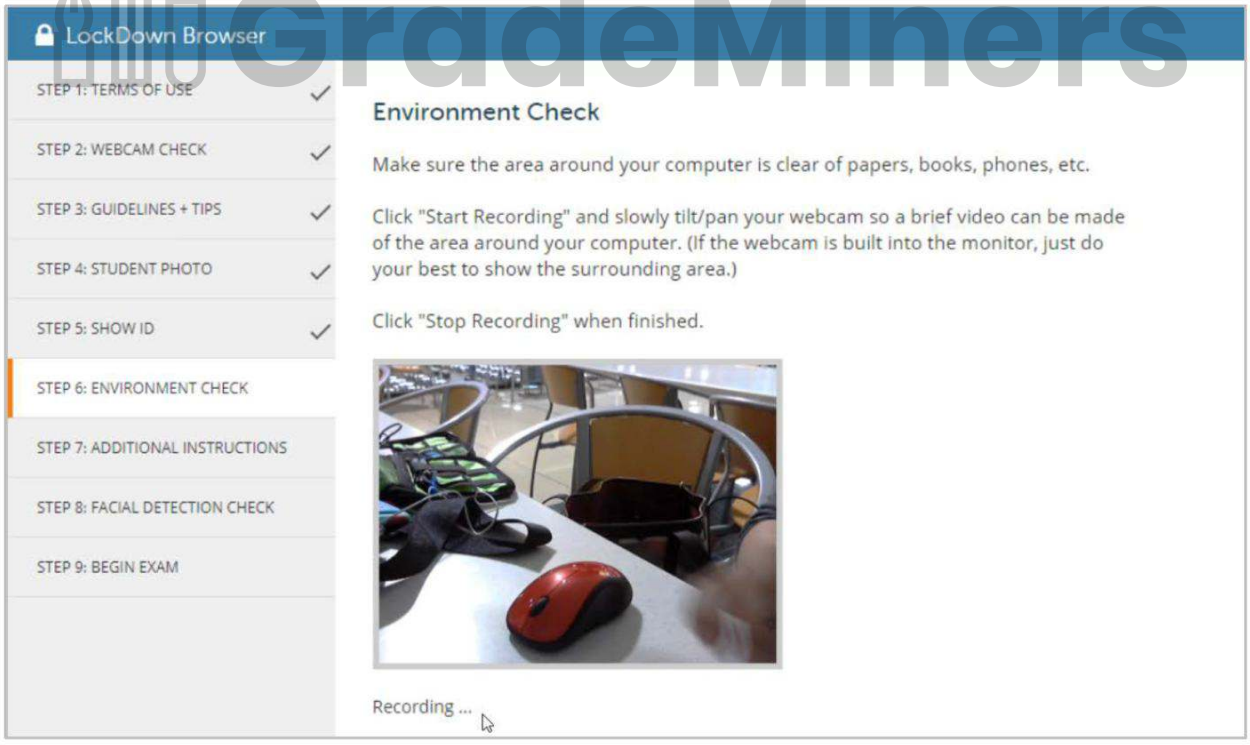

Figure 6: Step 6 of Installing Respondus Lockdown Browser

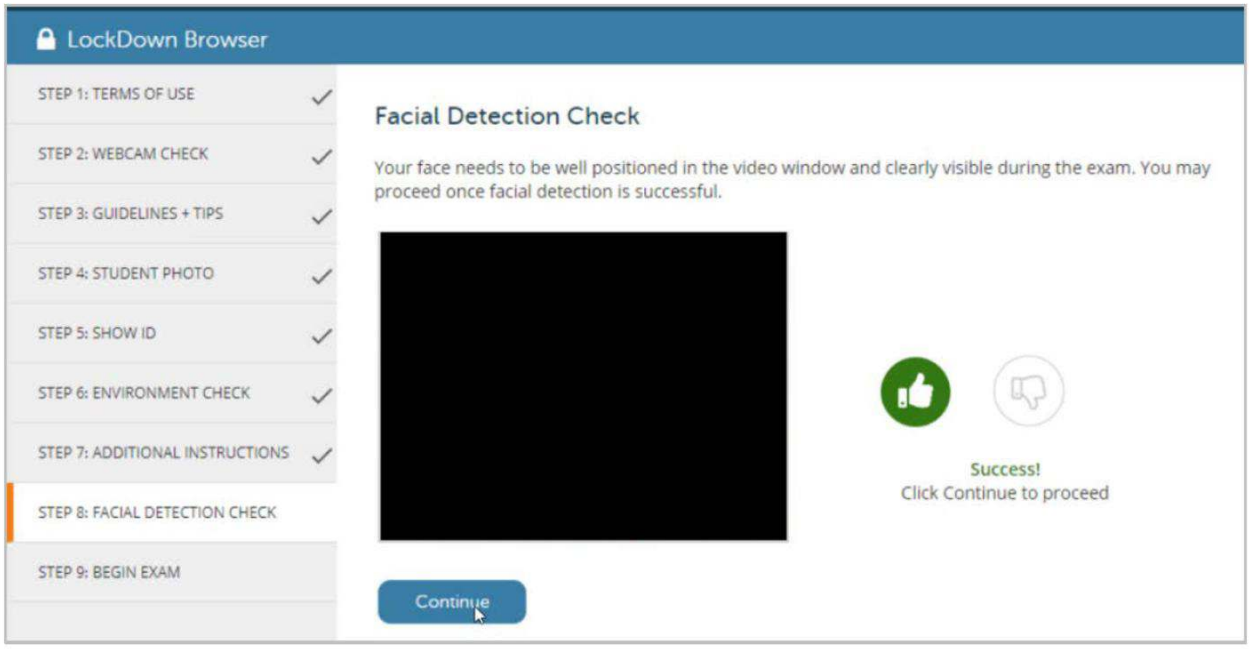

Figure 7: Step 8 of Installing Respondus Lockdown Browser

As mentioned earlier, the variables that were collected from these four lockdown browsers include their features, functionality, and settings.

Respondus

Respondus Lockdown Browser is compatible with a range of operating systems, including Windows, Mac, iOS, and Chromebook, ensuring flexibility in its use. However, for security reasons, it is not intended for use within a virtual machine. In terms of web browser compatibility, Respondus Lockdown Browser works seamlessly with Firefox and Chrome. Moreover, it offers integration options with popular learning management systems such as Blackboard, Schoology, Moodle, Canvas, and Sakai. Once installed, Respondus Lockdown Browser enforces several restrictions on a computer to maintain a secure testing environment [42]. These restrictions include:

- **Full-Screen Display**: Assessments are displayed in full-screen mode, preventing them from being minimized or obscured.
- **Simplified Browser Interface**: Browser menu and toolbar options are streamlined, retaining only essential functions like Back, Forward, Refresh, and Stop.
- **Enhanced Security Measures**: It prevents access to other applications, including messaging apps, screen-sharing tools, virtual machines, and remote desktop services, ensuring a focused testing environment.
- **Limited Printing and Screen Capture**: Printing and screen capture functions are disabled, preventing test takers from capturing exam content.
- **Copy and Paste Restrictions**: Respondus Lockdown Browser inhibits copying and pasting of content during assessments.
- **User Interface Constraints**: It disables right-click menu options, function keys, keyboard shortcuts, and task switching to prevent users from circumventing the lockdown environment.
- **Exclusive Access**: Assessments designed for use with Lockdown Browser cannot be accessed using alternative web browsers, ensuring the security and integrity of the testing process [42].

ProctorU

ProctorU, on the other hand, provides test-taking solutions through two distinct methods, allowing institutions to select the one that best aligns with their Learning Management System (LMS) integration preferences [2] [43]. These two methods include:

- **ProctorU Browser Extension**: This method is tailored for use with popular web browsers such as Firefox and Chrome. After installing the ProctorU extension, users

encounter an initial prompt that outlines the various actions it can undertake on their computer.

- **Guardian Browser Installation**: Alternatively, institutions may opt for the installation of the 'Guardian Browser' offered by ProctorU. The choice between the extension and the Guardian Browser depends on the institution's specific LMS integration requirements [2] [43].

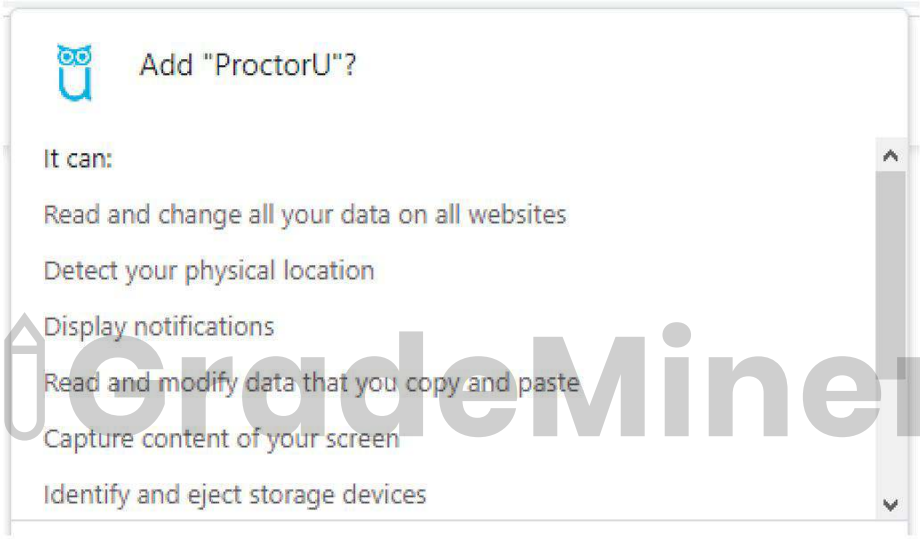

Figure 8: Installing ProctorU

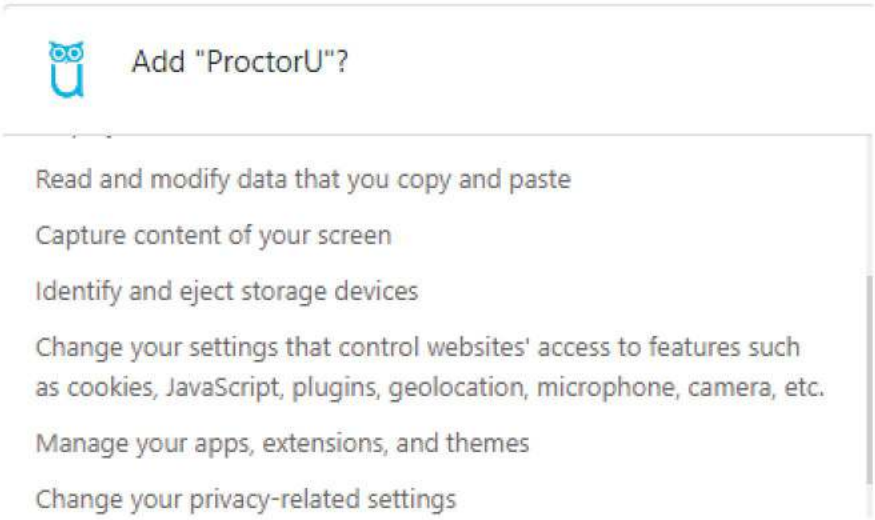

Figure 9: Installing ProctorU

Prior to the commencement of the test, a series of procedures are undertaken by both the product and proctors. These procedures encompass:

- **Biometric Data Collection**: Gathering biometric data from test-takers, providing a comprehensive 360-degree view of their testing environment.
- **User Consent**: Obtaining the test-taker's consent to remotely access their computer. This remote access is crucial for ensuring the absence of unauthorized resources or applications, which can pose a significant risk [2].

To facilitate these tasks, the service of choice is the GoTo platform, formerly recognized as LogMeIn. GoTo is a Software as a Service (SaaS) solution utilized for various purposes, including retrieving system information, enabling remote control, and deploying device configurations [43].

Upon successful installation of the extension, it is granted specific default permissions, including the ability to:

- Read and modify data on all websites.
- Detect the physical location of the device.
- Access and modify copied and pasted data.
- Capture screen content.
- Identify and eject storage devices, among other functions [2].

In accordance with their data retention policy, the data collected during test sessions is retained. However, it's essential to note that ownership of this data remains with the respective institutions. The duration of data retention is determined by the institutions themselves, with an automatic deletion occurring after one year, adhering to the guidelines outlined in NIST 800-88 [43]. This data is securely stored on servers located in the United States.

Inside the folder, there is a 'Manifest' text file that provides information about the types of data it collects from the user's computer. This encompasses various elements such as cookies, notifications, browsing data, clipboard read/write activity, desktop capture, and system CPU and memory usage, among other things.

Proctorio

Proctorio incorporates a range of features that are aimed at maintaining academic integrity during online exams. The features mainly revolve around the browser's ability to monitor, control, and restrict students' actions during the examination process. Some of the main features and functionality of Proctorio include behavioral monitoring, identity verification, content analysis, environment scanning, audio and video recording, advanced security settings, and data storage [44] [45]. Proctorio uses advanced algorithms to monitor students' behavior during online exams, which includes tracking eye movements, facial expressions, and head

movements, with the aim of identifying suspicious or irregular activities, which might indicate cheating. These algorithms are, nonetheless, proprietary and not publicly disclose [44]. The browser also uses various methods to verify the identity of the students taking the tests through such means as photo identification and facial recognition technology. From the analysis that was conducted, it was noted that these features help in ensuring that the test takers are indeed the registered candidate.

Proctorio can perform content analysis to check for unauthorized materials and/or resources within the exam setting by scanning the screen, browser tabs, and other applications that are running during the exam. It also captures and analyzes the surroundings via webcams to ensure there are no prohibited materials or individuals in the vicinity; this includes recording both audio and video, which allows proctors/educators to review exam sessions for any potential breaches to academic integrity [45]. For the settings, Proctorio comes with security settings, which restrict students from copy-pasting or printing exam content. It further disables certain keyboard shortcuts and prevent access to unauthorized websites or application. According Proctorio's official website, the data they collect is stored in secure servers, typically within the U.S., which is subject to the institution's data retention policies. The ownership of the data normally rests with the educational institution using the online proctoring tool [45]. The features are illustrated in the figures below.

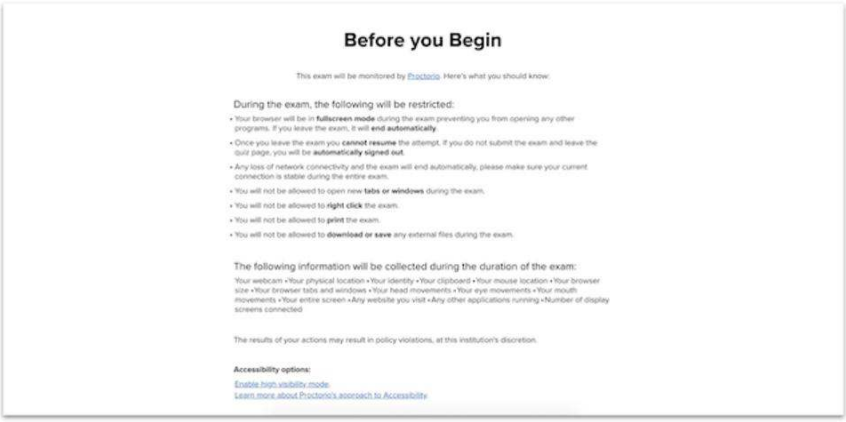

Figure 10: Detail Technical Overview of What Will be Accessed and Restricted

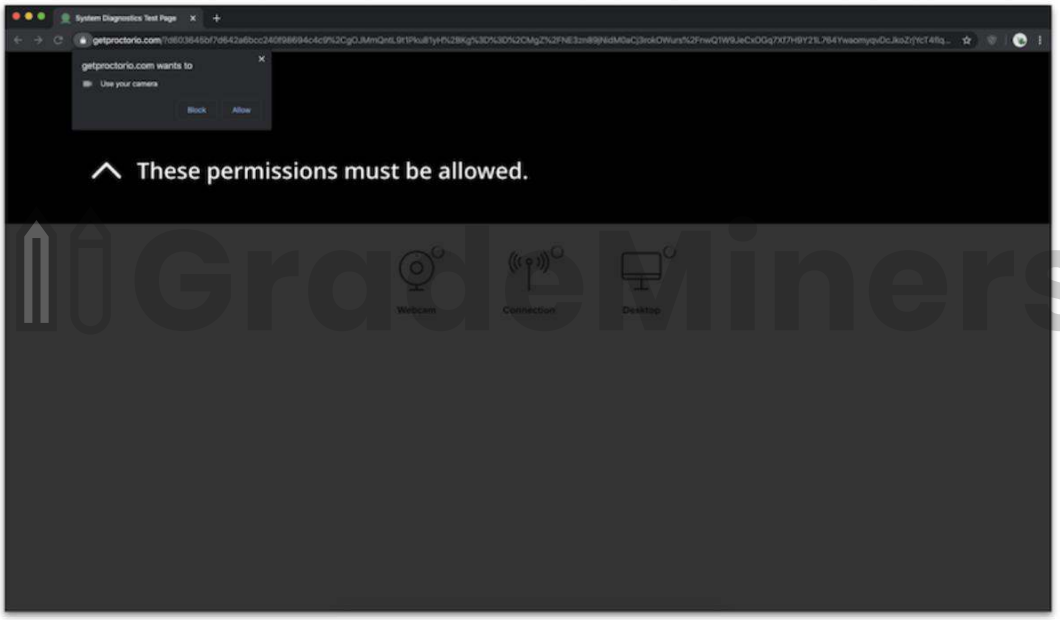

Figure 11: Access to Computer's Webcam Enabled

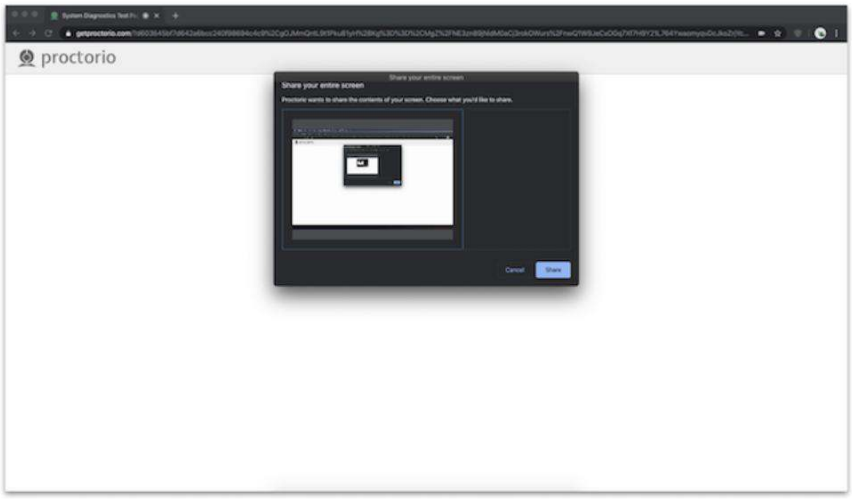

Figure 12: Screen Recording Enabled

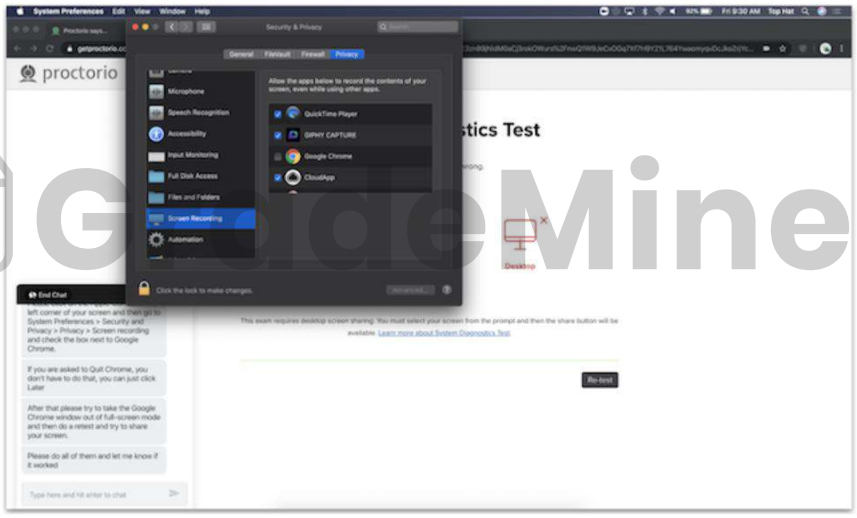

Figure 13: Screen Recording Enabled

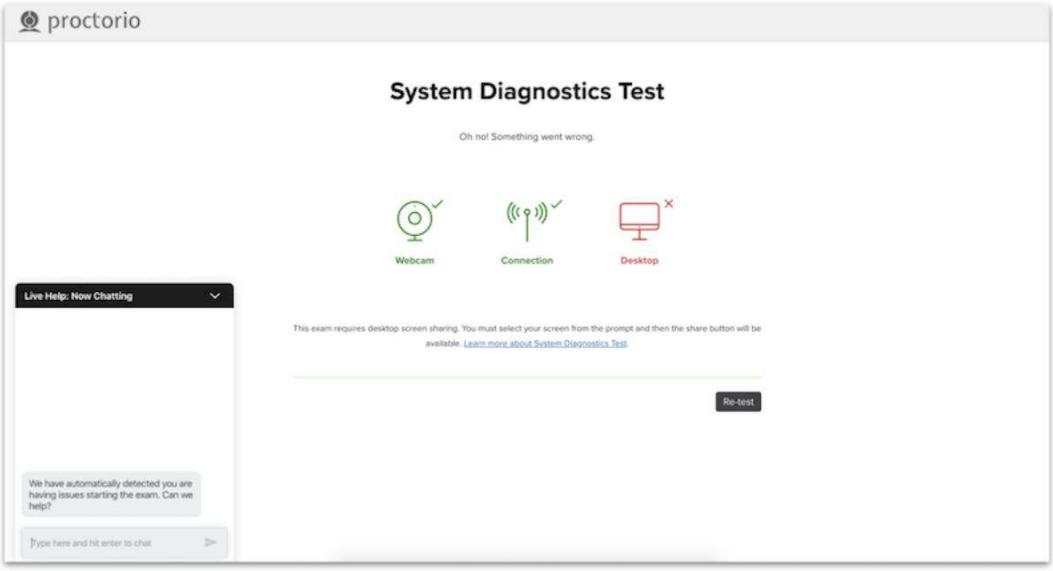

Figure 14: Live Chat for Troubleshooting

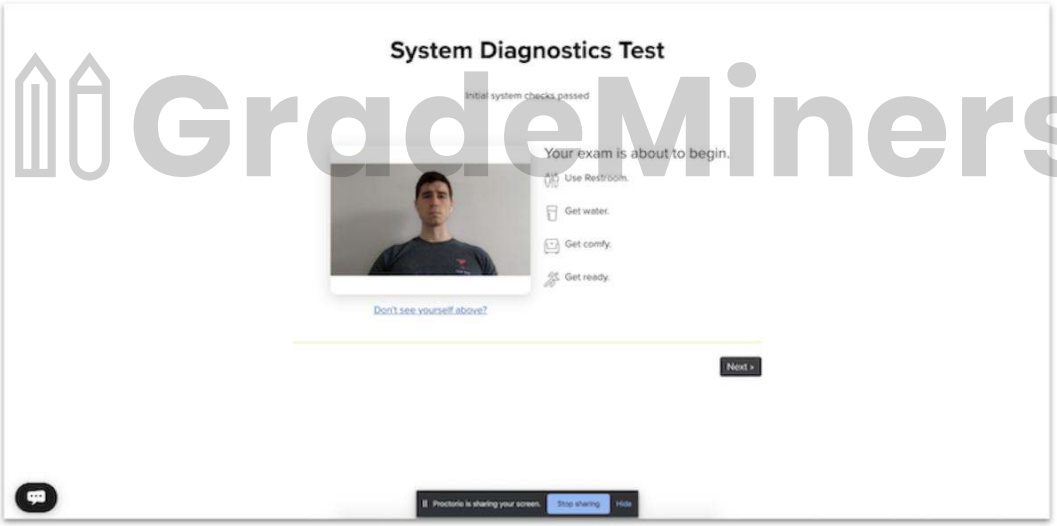

Figure 15: Preparedness Suggestions

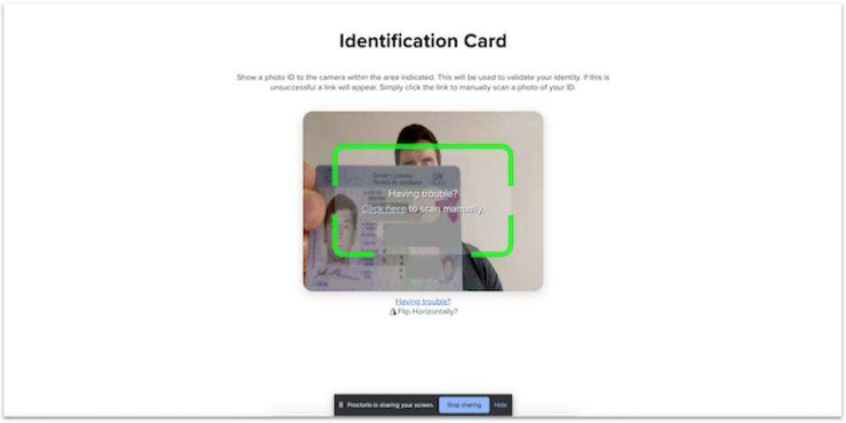

Figure 16: ID Verification

Figure 17: ID Verification

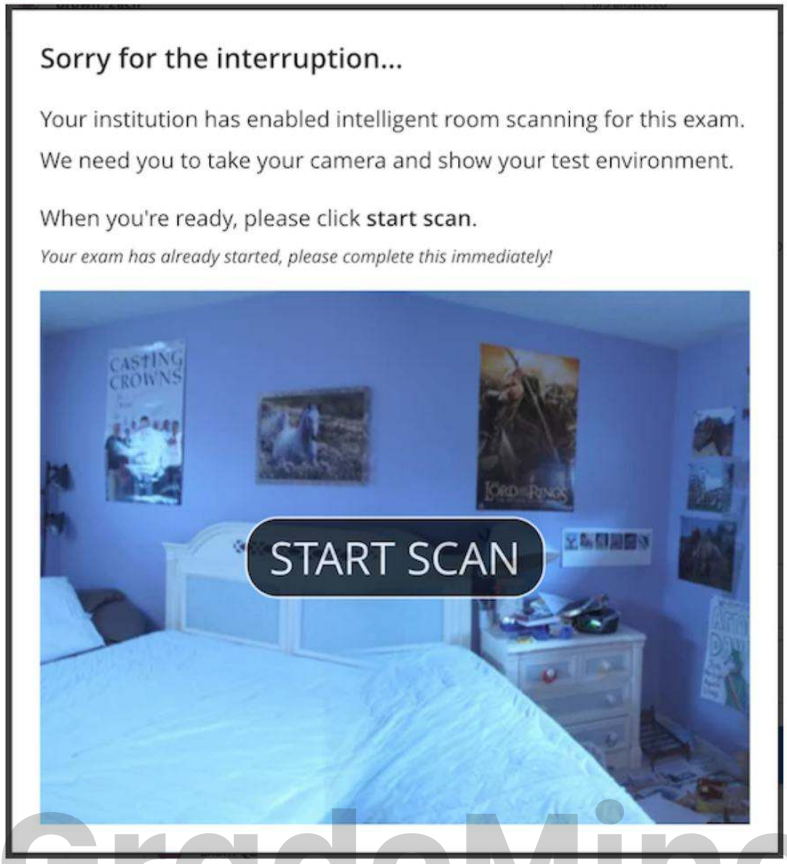

Figure 18: Room Scanning

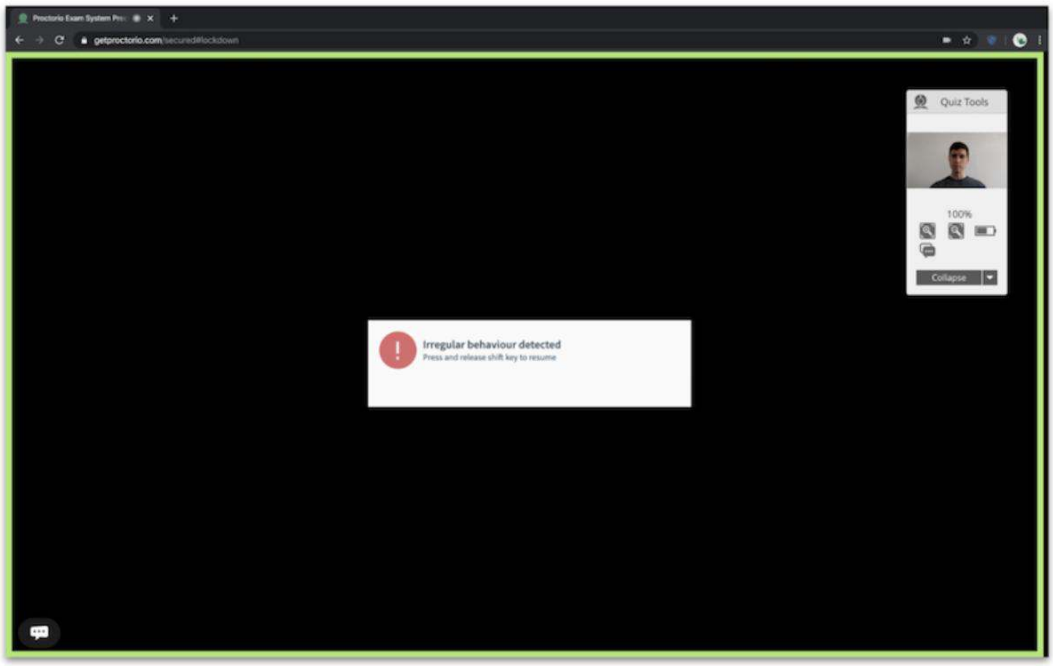

Figure 19: Flagging of Irregular Behavior

Examity

The main features and functionality of Examity, compared to the other three online proctoring tools that have been mentioned in this research paper include biometric authentication, live proctoring, secure browser, environment scanning, and customization. Examity employs such biometric authentication features as facial recognition and fingerprint scanning to verify students' identity prior to the start of the exams [46]. Examity, unlike Respondus, ProctorU, and Procotrio, normally offers live proctoring services where a trained proctor monitor students in real-time during examinations. This allows them to intervene in case suspicious behavior are detected. Respondus, ProctorU, and Procotrio heavily depend on automated proctoring [47]. The online proctoring tool also offers a secure browsing environment, which limits access to external websites, applications, and/or resources during exams. It also presents users more advanced settings to block specific functions.

Students are required by Examity to use their webcams to scan their testing environment prior to the start of the exam, which helps in ensuring a clean and secure testing space [46] [47]. It also allows institutions that use them to customize the proctoring settings according to their specific needs. Such flexibility can be advantageous in tailoring the proctoring experience.

Comparison of Features, Functionality, and Settings

Table 1 below summarizes the main features, functionality, and settings of the online proctoring tools being discussed in this research:

Table 1: Comparison of Features, Functionality, and Settings

Feature	**Respondus**	**Proctorio**	**ProctorU**	**Examity**
Biometric Authentication	No	Yes (Facial Recognition)	Yes (Facial Recognition)	Yes (Facial Recognition, Fingerprint)
Live Proctoring	No	No (Automated)	Yes (Live Monitoring)	Yes (Live Monitoring)
Secure Browser	Yes	Yes	Yes	Yes
Environment Scanning	No	Yes	No	Yes
Customization	Limited	Limited	Limited	Extensive Customization
Access Controls	Yes (Browser Lockdown)	Yes (Browser Lockdown)	Yes (Browser Lockdown)	Yes (Browser Lockdown)
Proctoring Settings	Limited	Customizable	Customizable	Customizable

Data Storage & Retention	Varies	Configurable	Varies	Configurable
Reporting & Analytics	Limited	Extensive Analytics	Limited	Customizable Reporting
Terms of Service / IP	Yes. Separated terms for student and instructors	ProctorU only uses the data captured during test sessions to conduct online proctoring	Proctorio cannot decrypt the audio, video, screen recordings and images collected and stored by Proctorio.	Examity does not sell, share, or market your data to third-parties.
Privacy Terms	User activity data is to improve the service; not sold to third parties, but shared with "partners" who provide data management solutions	User activity data is to improve the service; not sold to third parties, but shared with "partners" who provide data management solutions	User activity data is to improve the service; not sold to third parties, but shared with "partners" who provide data management solutions	User activity data is to improve the service; not sold to third parties, but shared with "partners" who provide data management solutions
Security Terms	Respondus reserves the right at all times to disclose any information or data stored by Institution, students or any other user as necessary, to comply with the law, a regulation or a governmental request, or to edit or remove any information or data	ProctorU may not directly or indirectly use, collect, disclose or destroy any Personal Information for any purposes that are not authorized by the University as specified in the Contract.	Data breach risk protection is not described in detail	Data breach risk protection is not described in detail

FEPRA Compliance	Yes	Not explicitly stated	Yes	Yes
Data Sharing	No	No	No	No
Outside Ownership of Any Part of Data Management	Blackboard Learn, D2L, Brightspace, Canvas	Not explicitly stated	Not explicitly stated	Not explicitly stated
User Consent	Yes	Yes	Yes	Yes

Privacy Implications and Ethical Dilemmas of Using Lockdown Browsers

The COVID-19 pandemic disrupted the delivery of education considerably, including the shift to online assessments and tests. As argued by Janke et al. [51], evidence indicates that there is in-creased academic dishonesty especially in unsupervised online testing, which prompted academic institutions to implement online proctoring interventions. On one hand, the results of this study acknowledge that academic dishonesty increases in situations such as non-proctored online learning. On the other hand, however, it is also noted that there are concerns about the consequences of online proctoring on the privacy of students. Chen et al. [26] asked higher education students if they had reservations about their schools collecting and storing their personal data. The responses suggested that a significant majority of the students had confidence in their institutions to safely handle their data particularly if the institutions used branded and proven institutional apps. However, consistent with findings by Janke et al. [51], Chen et al. [26] also found that the students extremely concerned about third-party tools and how they use and manage their personal and sensitive data. The students expressed concerns that their schools do

not prioritize selecting secure and reliable educational technologies that can ensure their personal data is kept safe.

As it has been established in the study and discussed below, the lockdown browsers record the examinee and their environments throughout the testing period. Essentially, this recording constitutes a violation of the examinee's privacy. Study findings [3] [18] [22] indicate that students' information obtained when student data is processed by lockdown browsers are used for purposes such as targeted marketing and advertising by for-profit companies. Additionally, algorithms process the examinees' online behavior and communications discretely, after which the data is aggregated to generate profiles about them. For example, Gribbins and Bonk [3] have shown that people's identities in the modern information age are increasingly becoming digital and as students engage with online proctoring tools, their private online lives fuse with their academic courses. The personal data that constitute their identities are usually disclosed inadvertently, exposing students to the misuse of their private and personal data.

According to its developers, Examity's audience includes test administrators, evaluators, and examiners who seek an AI proctoring software solution to manage online exams [5]. Examity uses AI to complement software and provide automated proctoring. Academic institutions can choose between automated or standard proctoring with auto authentications. Further, since the academic institutions have the ability to fully configure the process, they essentially have full control over the authentication process. Once the proctoring session ends, a complete video recording of the testing is sent to the Examity dashboard, including time-stamped comments, to be reviewed by the exam administrator. ProctorU is another software-only proctoring tool for identity verification and proctorless testing sessions. It is marketed as a solution for academic institutions that seek to protect the integrity of online exams [19]. Its

developers claim that it not only detects, deters, and prevents academic dishonesty but also validates knowledge, reduces the cost of administering online exams, and expands access to remote students. The software is an additional level of deterrence that records the exam session, which is then reviewed by exam administrators to identify suspicious behavior.

Proctorio targets K-12, higher education, federal agencies, and corporate clients to offer identity verification and proctoring services for exams [1]. Compared to other proctoring tools, Proctorio's bandwidth requirements are the lowest and it is marketed as a proctoring tool that gives priority to the examinees' privacy and security because it uses end-to-end encryption. Additionally, the browser's extension integrates with most of the learning management systems and third-party exam platforms used by most of the academic institutions. Proctorio offers a set of lockdowns, recording, and verification features that allow the exam administrators to tailor exams for the respective degree of exam security. Respondus is designed for academic institutions that seek fully automated proctoring to deter academic dishonesty in online exams. The browser uses the examinee's webcam and video analytics to prevent dishonesty in non-proctored exams. Respondus conducts a second-by-second analysis of the entire exam session using facial detection and motion and light analysis of the environment in which the exam is being taken. It also uses data from the examinee's computer to identify irregularities and patterns associated with academic dishonesty. Such data includes hardware changes, keyboard activity, and mouse movements.

This research has found that one consequence of online schooling is the increasing use of lockdown browsers, which are used to administer exams in an experience similar to the traditional classroom environment to discourage and identify cheating. Although each lockdown browser has its own specifications and functional features, they share some commonalities. For

example, it has been shown that the lockdown browsers lock down the browsers on the examinees' computers and prevents them from opening other applications [30]; the lockdown browsers record all mouse movements, keyboard strokes, hardware changes, and uses AI to identify suspicious conduct [22]; the lockdown browsers use the webcam and facial detection technology to compare the examinee's image with a photo ID or a photo taken on the website [36]; the facial detection feature tracks the examinee's eyes and body movements in an attempt to detect suspicious patterns that may indicate cheating [15]; the lockdown browsers also detect changes in lighting and analyze the examinee and their surroundings [10]. According to Ismail et al. [12], the above functions of a lockdown browser are a major violation of the student's privacy and security, which is also compounded by the fact that the student is not fully informed of how the lockdown browser functions or how the data it collects will be used. Equally importantly, it has been found that proctoring companies share the students' information they collect with their third-party business affiliates.

This study has established that remote learning has become common and is gaining popularity alongside the traditional classroom. More specifically, online examinations are increasingly being used to test students remotely, the implication of which is that the need for the physical presence of invigilators or proctors has been reduced. On one hand, the need for online examinations has been created by the advent of emergency conditions, the most notable of which is the COVID-19 pandemic, which make it impractical to use the traditional classroom setting. Further, the concept of globalization has made it possible for people around the world to complete academic courses and take examinations from remote locations without necessarily having to be physically present in a classroom. On the other hand, however, there are issues associated with the technologies such as lockdown browsers used to administer the examinations

under such circumstances. As this study has found, the privacy and ethical dilemmas associated with the use of lockdown browsers primarily include invasive monitoring, data security, privacy of home environment, lack of control, data retention and sharing, and nonacademic use of student's data. Respondus, for example, disables the examinee's functions such as printing, copying, accessing other applications, or going to other URLs. Generally, lockdown browsers such as Respondus, Examity, ProctorU, and Proctorio feature applications that require examinees to record themselves throughout the entire test period, and they also capture a full view of the environment in which the test is being taken. As acknowledged in the literature review [15] [26] [43], lock-down browsers essentially let themselves into the examinees' living space and this has considerable consequences. For example, Chen et al. [15] note that not only are the lockdown browsers invasive physically and technologically but they also create unequal testing experiences compared to those of the classroom. Further, Chen et al. [26] argued that proctoring tools are an unnecessary way of observing students. Similarly, Dadashzadeh [43] reported that a significant majority of students expressed lack of trust and confidence in lockdown browsers, which they described as prone to technical faults, a cause of anxiety, and an intrusive way of unnecessary surveillance. Equally importantly, Chen et al. [26] found that lockdown browsers do not offer an equal testing experience to examinees with physical disabilities.

Study results [2] [31] [37] show that a lockdown browser is ideally an invasive malware through which school administrators and their third-party software vendors can violate the privacy rights of students and expose them to consequential security threats. In that context, Nigam [42] reported that educational institutions are also exposing themselves to class action for data breaches by compelling examinees to install surveillance software on their computers. For example, Khalil et al. [2] demonstrated that a history of security violations in proctoring tool

vendor is a major security concern after ProctorU confirmed in August 2020 that more than 400,000 records were not only stolen but also publicly leaked. Similarly, Ziede [6] found that while the need for proctoring tools is acknowledged, they also cause more harm than the expected benefits especially in terms of the examinees' privacy. Respondus, for example, records the examinee's movements and audio, which is essentially and invasion of their privacy [6]. While the need for lockdown browsers is acknowledged, Lee and Fanguy [8] and Ahmad et al. [14] argue that the harm they cause outweighs the benefits primarily because of recording videos and audios of the examinee. Terpstra et al. [18] also explained that the students have personal lives that they may not have full control of. Family members, for example, are not always aware of the student's situation and could inadvertently com into view of the webcam while the student is in the midst of an exam. As Terpstra et al. [18] observed, software such as Respondus will automatically report such accidental appearances by family members as suspicious activity, which is not only an invasion of the student's privacy but also that of their family members and friends.

Respondus articulates its terms and conditions on their website, essentially excluding themselves from any accountability in the event that the examinee's privacy and data confidentiality are breached. More specifically, Shaak [22] cites the claim that by agreeing to the terms and conditions of Respondus, the examinee uses the software at their own risk and the company will not be responsible for malfunctions or the mismanagement of student data. As Shaak [22] argues, it is unethical for the software company, the academic institution, and any other third-party to compel students to use the software and not offer legal recourse in case of privacy violations. Yet, consistent with, Huber et al. [28], this research finds that the lockdown browser developers prioritize academic integrity over respecting the examinee's privacy and

protecting their sensitive information such as login details, IP address, birthdate, location, name, and the privacy of their homes.

This study has documented a period when lockdown browsers were established initially as a short-term emergency intervention but trends show that they might be retained and used more frequently in future. In the post-COVID-19 era, online proctoring is acknowledging as a necessary technology for academic institutions. As argued by Balash et al. [36], in an institutional context, adopting a data-driven system of remote exam administration is viewed as practical approach towards catering to a remote customer base. However, while online proctoring is arguably good from a business perspective, its privacy implications can be criticized. The concerns raised through the initial protests, for example, reveal valid issues that need to be addressed. Balash et al. [36] demonstrated that despite the benefits of modern technology, normalizing facial analysis as well as other forms of automated biometric monitoring through online proctoring as part of teaching and testing brings forth a concerning precedent. Equally importantly, the outsourcing of essential educational functions to commercial applications aggravates the current trend of subjecting learners to pervasive forms of monitoring and data collection. There is general consensus among commentators [43] [44] [45] that the intrusion by software vendors and outsourced personnel into the pedagogic roles creates issues about the consequences of commercializing education. Further, Davis et al. [45] argued that the distanced forms of provision that are characteristic of online proctoring are disrupting the conditions of administering exams considerably.

According to Harwell [44], if academic institutions must continue using online proctoring tools, it is also critical that new rules and ethical guidelines are formulated at the policy level and enforced at the practice level. Such rules and ethical guidelines should reflect the best values of

academic conduct and, more importantly, respect the students' privacy and dignity. It is important that online proctoring tools are developed in light of decent morals, ethics, and political intent to contribute positively to the quality of education rather than subject students to stressful experiences while collecting their personal and sensitive data. It is important that academic institutions make their processes of procuring online proctoring tools more consultative and democratic while the technology developers and vendors act in more ethical and respectful ways when the engage with educational products [43]. Similarly, Davis et al. [45] also argued that online proctoring tools should be considered as a warning that the academic fraternity needs to develop counter-narratives against the envisioning of education as a technology issue. Rather, administering exams remotely should be viewed as a social concern, whereby students' right to privacy is prioritized.

Summarily, it has been shown that the proctoring tools used by academic institutions are a privacy risk not only to the examinees but also their families. On one hand, educators are encouraged to embrace technology but, on the other hand, the policies in place to protect both the students and educators are insufficient, creating a dilemma between technology and privacy. Statis-tics show that 96% of the proctoring tools currently in use share the students' personal information with third parties [46]; 79% of the information shared is used for commercial purposes such as advertising and data analytics [47]; 28% of the proctoring tools use the information they gather for non-academic purposes [46]; and the information is typically shared without the students' knowledge and consent [47]. It has also been found the advertisements placed on proctoring websites create additional opportunities for marketers who use re-targeting advertising campaigns and, more importantly, cookies and search history [1].

Ethical Dilemmas

This study has found previous research that has highlighted the considerable attack under which the ethics of automated proctoring have come against, not only from students but also their parents and faculty. Rao [38], for example, found that students report heightened levels of anxiety when they are subjected to proctored online exams the invasive monitoring of lockdown browsers, raising concerns about their data and privacy rights. Some university students also launched petitions against their institutions arguing against the use of automated proctoring especially with regards to violating their privacy rights [38]. However, the universities and technology vendors have responded by arguing that the lockdown browsers use encryption software and that the data they gather is not sold to third parties. Considering that educational technology companies have previously been found to publish or even monetize students' personal data, Price and Cohen [37] argued that privacy concerns in the digital age are particularly more legitimate now than ever before, especially from an ethical perspective.

This study acknowledges the growing popularity of online proctoring, which has enabled students to sit for their certification exams remotely. It is worth noting that literature [1] [17] [22] highlight the benefits of online proctoring, such as convenience, flexibility, cost-effectiveness, and efficiency. For example, Shaak [22] describes online proctoring as convenient because it eliminates the need for examinees to travel to testing centers, especially for those from remote locations or with limited transportation options. Bergmans et al. [17] explained that online proctoring also offers examinees flexible schedules for their exams, whereby they can select dates and hours that fit best in their routines. Further, the elimination of physical test centers renders online proctoring more cost effective compared to traditional proctoring approached because it reduces the costs associated with administering exams [1]. According to Hussein et al.

[1], online proctoring also increases the efficiency of administering exams because the tests are not only graded automatically but the results can also be ready immediately upon completion [17]. However, as demonstrated by Holden et al. [9], Ahmad et al. [14] and Chen et al. [15], online proctoring is in itself not the problem per se; rather, it is the need for the technology used, especially lockdown browsers, to collect personal information for authentication purposes that brings forth privacy concerns.

Studies [9] [14] [15] show that the use of lockdown browsers has given rise to ethical dilemmas that challenge academic institutions, legislators, and policymakers with regard to the potential to breach students' privacy rights. Poll results by Gudiño Paredes et al. [10] show that parents, learners, and third-parties are not comfortable with the requirement for students to be subjected to webcam surveillance, which they described as intrusive especially when the exam is being taken from home. Quintel and York [25] also identified another ethical issue in the form of worsening social and economic disparities among student. For example, they showed that lockdown browsers affect students disproportionately in some situations, such as when some students have limited or unreliable access to technology and the internet. This is inferred to mean that students from lower socioeconomic classes may not always have the required resources such as computers and internet connectivity, which essentially creates a considerable ethical dilemma. Further, the use of biometric data such as fingerprints and facial recognition also raises data security and privacy concerns [10].

Chen et al. [15] reported that online proctoring is not always culturally sensitive; it potentially brings forth issues for students from diverse backgrounds. This view is also supported by Chen et al. [26], who contended that some students, for example, belong to cultures that view direct eye contact as rude; yet, the lockdown browser may flag the examinees' avoidance of

looking straight into the webcam as suspicious behavior. Chen et al. [15] and Chen et al. [26] agree that none of the current online proctoring systems has been designed with the necessary cultural sensitivity to protect all students against unfair disadvantages. As established in the literature review, students are not fully informed of the process of online proctoring and, more importantly, their personal data that is collected and how it will be used or for how long the proctoring companies will store such data. Therefore, according to Nguyen et al. [53], the proctoring companies and schools do not make the ethical consideration of seeking informed consent from the students, which essentially compromises the transparency of the entire online proctoring exercise.

Other ethical concerns include the challenges in meeting accommodation requirements for students with disabilities and concerns with the possibility of gender and racial bias that has been identified as inherent in facial recognition software [45]. Proctors have the responsibility of monitoring examinees' behavior as they take exams to detect cheating; however, this study has found that such monitoring creates the potential for bias. Dawson [52], for example, reported that students have also expressed concern that the proctors' judgment may be swayed by their personal assumptions, beliefs, and biases, which could lead to unfair treatment of some candidates and ultimately incorrect results that undermine the integrity and underlying purpose of exams. Dawson [52] also found that online proctoring is not always accessible to all examinee and especially the physically disabled who may need accommodations such as alternative testing methods, additional time, and special equipment for them to take the exam. Considering that online proctoring and the associated lockdown browsers may not accommodate such requirements, the situation disadvantages some students and also violates anti-discrimination legislation.

From a technical perspective, Quintel and York [25] found that not all students can afford the necessary resources such as fast and steady internet connection, a functional computers, microphone, and webcam, yet they are required to take the same exams as those who can afford the resources for them to be certified. Such technical issues as software bugs, hardware malfunctions, and poor internet connectivity potentially disrupt exams and subject examinees to stress and anxiety. Although it has been argued that online proctoring reduces the cost of administering exams by eliminating the need for traveling to the testing center, Quintel and York [25] also argued that the cost of the online proctoring services and the required equipment is often passed on to the examinees. From an equity and accessibility perspective, this is an important observation because it creates an ethical consideration whereby the cost could create financial barriers that hinder some students from doing their certification exams.

The above results show that online proctoring and the use of lockdown browsers are necessary aspects of education in the modern information age. These educational technologies, however, come along with ethical considerations that policymakers and educators must address to ensure that online exams are characterized by integrity, fairness, and transparency. Before educational institutions decide to use online proctoring and subject examinees to the invasive monitoring of lockdown browsers, they must carefully consider their advantages and disadvantages from an ethical perspective. While technology continues to evolve, there is need for software developers and educational institutions to seek a balance between academic integrity and ethical principles. Although the responsibility to create a fair and transparent examination process is on the educational institution, it is also critical that software developers and online proctoring companies develop and implement technology that supports ethical considerations. To ensure the credibility and fairness of online proctoring and protect examinee's data privacy,

policymakers and legislators have developed laws that can be useful for website operators and educational institutions. These are explored in the following discussion of research question three of this study.

Table 2 below summarizes the main concerns (recurring themes) among students with regard to the use of online proctoring tools. The

Table 2: Summary of Key Concerns and Recurring Themes

Data Security ● Certain online proctoring firms retain students' recorded data for extended periods [15]. ● Remote proctoring service providers have encountered instances of data breaches [2]. ● Instructing students to install software that compromises the security of their digital environment might establish unfavorable practices related to data security [31].	**Hardly Prevents Cheating** ● Students have discovered methods to bypass proctoring software and share these workarounds publicly [49]. ● Real-world assignments offer a more practical evaluation of genuine skills, allowing students to be assessed in the most efficient manners [8].
Test Anxiety ● The use of remote proctoring systems may elevate students' stress levels [9].	**Accessibility** ● Some characteristics of remote proctoring systems might not align with adaptive technologies, like screen readers [15].

• Student academic performance can decline due to test-related anxiety [7].	• Obtaining fundamental access to these technologies is frequently challenging [11].
Bias – Race, Ability, Gender • Certain disabilities can inadvertently trigger cheating alerts, such as tics, eye movements, self-soothing behaviors, or the need for a break [11]. • Flagging these behaviors isn't a flaw but a deliberate aspect of AI proctoring systems, which are engineered to identify "unusual" actions [50]. • Algorithmic proctoring utilizes facial recognition/detection technology, which may have difficulty recognizing individuals with darker skin tones [24]. • Students might be locked out of exams if their face isn't detected in the frame [33]. • Seeking assistance may lead to disconcerting troubleshooting practices, like being asked to shine light on your face [30].	**Invasion of Privacy** • Room scans can be intrusive, potentially exposing personal information that students prefer to keep private [2]. • Some product features may require students to display parts of their bodies, like their lap, in ways that could be deemed inappropriate [45].

• AI identification methods can pose challenges for transgender and non-binary students [16].	
Cost • Proctoring expenses can reach over $500,000 annually [18]. • These high costs are often passed on to students or institutions facing financial constraints [42]. • Furthermore, there may be extra expenditures due to potential legal disputes and public relations concerns [9].	**Liability** • Compliance with state or local regulations on student surveillance and biometric data collection may not always be met by proctoring services [25]. • When students are engaged in course activities and have human proctors present, there may be concerns about potential harassment or harm [39].
Digital Divide • Some remote proctoring solutions necessitate costly hardware (e.g., laptops, webcams, microphones) that some students may not possess. They may also demand the installation of particular software components (e.g., specific browsers, extensions) that students might be unwilling to install [32].	**Larger Harms to Freedom and Society** • Surveillance technologies are employed alongside human rights infringements worldwide. The use of proctoring tools normalizes surveillance practices for students [50].

• Internet connectivity quality varies, and certain students may encounter difficulties with their internet connections [44].	

Regulations and Guidelines Governing Data Privacy in Educational Environment

The modern era is characterized by emerging technologies such as Internet of Things (IoT), artificial intelligence (AI), cloud computing, and algorithmic and analytic capabilities that are also finding use in the academic setting. As has been found in this study, academic institutions are making efforts to embrace technology designed to enhance teaching and learning by developing internal processes to protect the privacy of students and confidentiality of their data. However, it has also been found that academic institutions are yet to find the optimal balance between adopting technologies such as lockdown browsers and protecting the students' privacy. Alongside the growth of online teaching and learning tools are the inherent risks of exploiting students and invading their privacy. According to Weiner and Hurtz [23], the most obvious measure that can be taken to prioritize the privacy of students as they use proctoring tools is to enact laws and regulations and implement adequate enforcement policies.

Within the academic context, data privacy is governed by various laws, rules, and regulations as well as ethical guidelines, which could also be specific to certain jurisdictions. In the United States, for example, the Department of Education supports the protection of students' privacy by enforcing laws such as CIPA, COPPA, and FERPA as well as others that are specific to certain states. At the international level, there are laws such as the International OECD

guidelines, GDRP, and the International Baccalaureate (IB) Privacy Policy. Further, common law countries also derive laws from court cases. For example, US District Court judge Philip Calabrese ruled on August 22, 2022, that lockdown browsers are a violation of the 4th Amendment. This is consistent with arguments by Ziede [6], Weiner and Hurtz [23] and Mutimukwe et al. [24] that lockdown browsers violate students' right to privacy.

CIPA

CIPA is primarily concerned with children's access to harmful or obscene internet content. Therefore, it places responsibility on K-12 schools and libraries to implement measures such as web filters to protect children's online activities. This law applies to all schools and libraries that participate in the Federal Communication Commission's E-Rate discount program, through which the schools and libraries receive discounted rates to connect to and access the internet [24]. CIPA places certain responsibilities on the schools and services for them to be compliant. For example, they must demonstrate that they have internet safety policies for them to receive E-Rate discounts, whereby such protections must either filtering out or completely blocking Internet content that is deemed harmful or obscene to children. For the schools and libraries to prove they are compliant, they are required to publish their compliance policies and convene at least one public meeting [24]. Further, the schools and libraries are required to have measures to monitor children's online activities and, in accordance with the Protecting Children in the 21st Century Act of 2012, educate the children on how to conduct themselves online. CIPA also requires education curricula to include suitable online interactions in chat rooms and on social networking and also cyberbullying and response.

CIPA best practices that ensure compliance with the law include posting notifications and being transparent. As explained by Ziede [6], federally funded schools and libraries should use

both electronic and physical signs to notify users that they have installed filtering software in compliance with CIPA. With regards to transparency, the institutions should post signs notifying users whenever they have turned off filters [6]. For example, Weiner and Hurtz [23] reported that filtering software is sometimes not accurate and could, therefore, wrongly block some useful sites. However, CIPA allows the institutions to unlock such mistakenly blocked sites when they are proved to be legitimately necessary for educational purposes, but the institutions should notify users of such unblocking.

FERPA

FERPA is a federal law designed to protect students' data privacy by granting their parents some rights to the records until they (the students) are eligible to own the right to their records [24]. As a federal law, FERPA applies to all schools and universities and educational agencies that are funded by the US Department of Education. FERPA covers all student education records, whereby the law defines student education records as all the records that relate directly to the student and are maintained by their educational institution or agency. As Ziede [6] reported, such records include those of children with disabilities as defined under Part B of IDEA (Individuals with Disabilities Education Act). However, the definition of student education records under FERPA exclude law enforcement unit records as well as any other documents retained by the school resource officer or any other law enforcement agencies [6].

Under FERPA, the right to obtain and possess student data transfers to the student once they reach 18 years of age or enroll into an educational institution higher that the high school level, whereby they are then referred to as eligible students. Before the educational institution can share any of the student's record, they must receive written consent from the eligible student or their parent [6]. Nonetheless, there are certain conditions under which the educational

institutions can share students' records without the students' or their parents' permission. These include complying with a subpoena or court order; when needed by school officials with genuine academic interest; for purposes of accreditation; when needed for evaluation purposes, financial assistance, and audit; in the event of safety and/or health emergencies; and when needed by state or local authorities within the juvenile justice system [6]. Schools also do not need the students' consent to disclose their directory information, which include their names, date of birth, telephone number, address, attendance dates, and awards and honors [6]. FERPA places certain responsibilities on schools for them to be compliant. For instance, the schools are required to inform eligible students and parents each year of their rights under FERPA. They are also required to inform eligible students and their parents about directory information and allow them reasonable time to request for non-disclosure [6].

FERPA best practices that ensure compliance include vetting all learning tools, implementing basic security measures, and transparency about data collection. With regards to vetting learning tools, Weiner and Hurtz [23] proposed that institutions should have policies for vetting tools associated with educational technology, which will allow the learners and their instructors to know the sites, platforms, and apps that have been certified as safe for learning. Additionally, the Department of Education encourages the collaboration between legal counsel and IT resources in institutions to vet educational technology tools for FERPA compliance [23]. At the minimum, studies [23] [24] have shown that institutions should adhere to basic cybersecurity practices such as identifying authorized and unauthorized resources; implementing role-based access to personal information and reviewing them on a needs basis; encouraging the use of virtual private networks on unsecured connections; and teaching cybersecurity measures such as the use of strong passwords, signing out of unattended devices, and staying aware of the

threat of malware and phishing attacks. On being transparent about data collection, it has been noted that institutions are required by FERPA to notify eligible students and their parents about their rights every year [23]. To improve compliance, the Department of Education recommends that institutions inform eligible students and parents of the data that they collect and how they will be used, and this also applies to information that is not subject to FERPA privacy protections or any other student privacy laws.

COPPA

The Federal Trade Commission (FTC) has prioritized the protection of children's online privacy since 1998 when it proposed that Congress pass legislation that puts parents in control of the online gathering and use of their children's personal information by website operators. Essentially, the FTC is committed to guaranteeing that education technology tools and the potential benefits they offer do not lead website operators to overlook the need to protect children's privacy rights. As Mutimukwe et al. [24] explained, the FTC intends to enforce COPPA's requirements for limiting website operators' ability to gather, use, and retain children's data and this also includes in academic institutions where parents are often concerned by the lack of alternatives. It is noted that since COPPA was enacted, there has been a steady emergence of technologies that allow the online collections and commodification of consumers' personally identifiable information (PII). More importantly, Mutimukwe et al. [24] has argued that there is also an increase in the number of business entities that rely on the monetization of their consumers' PII. Further, the rise of targeting practices based on the collection of consumers' activities on the Internet has also created concerns that businesses could engage in harmful practices, and this necessitated the reinforcement of children's privacy safeguards [24].

Study findings Ziede [6] and Weiner and Hurtz [23] show that the FTC responded to these concerns by revising COPPA, effectively holding third parties liable for collecting children's PII from child-directed websites in violation of the law. Such third parties include advertising networks such as Google LLC and YouTube LLC. The courts have also used COPPA to find the advertising networks in violation of children's privacy rights in cases such as *United States v. OpenX Techs., Inc.*, Case No. 2:21-cv-09693 (C.D. Cal. Dec. 15, 2021); *FTC and the State of New York v. Google LLC and YouTube, LLC*, Case No. 1:19-cv-2642 (D.D.C. Sept. 4, 2019); and *United States v. InMobi Pte Ltd.*, Case No. 3:16-cv-3474 (N.D. Cal. June 22, 2016). In these cases, the definition of PII was expanded to include persistent identifiers that are used by advertising networks to target children in their advertisements.

COPPA was enacted in light of the concerns about data collection in the school context, where students and parents are often required to engage with education technology for them to participate in activities related to academic requirements. However, Ziede [6] has argued that the school-issued devices that students use also allow the collection of even more PII, which is then shared with third parties. To that end, FTC personnel developed a comprehensive guidance on the application of COPPA to education technology vendors. The guidance covers the prohibition against mandatory data collection; prohibitions on the use of the collected data; prohibitions on the retention of the collected data; and security requirements. The prohibition against mandatory data collection requires COPPA-covered entities, including education technology vendors, not to condition the participation of children in any activity on them disclosing more information than what is reasonably needed for such participation [6]. It follows, therefore, that the entities cannot bar students/children from using education technology if they do not disclose information that is beyond what the administrators need to facilitate their participation.

Under the prohibitions on the use of the collected data, COPPA places strict limitation on covered entities, including education technology vendors, on how they can use the PII gathered from children. As Weiner and Hurtz [23] explained, education technology operators can only use the PII they collect to deliver online education services; they are not allowed to use such PII commercially for purpose such as advertising and marketing or any other non-academic purposes. COPPA's retention prohibitions also bars covered entities from retaining children's PII for any longer than they reasonably need to perform the purpose that they collected the information for [23]. Finally, COPPA's security requirements compel covered entities to implement procedures necessary for the maintenance of the children's data's integrity, confidentiality, and security [23]. This is important because, even without an actual data breach, COPPA-covered entities will be in violation of the law if they do not have reasonable security measures in place. Overall, the limitations on the gathering, use, and retention of children's PII, alongside the security requirements, obligate covered entities to implement strong privacy safeguards. Notably, the responsibility for compliance with COPPA is on education technology businesses and not academic institutions or parents.

COPPA best practices that ensure compliance should include having a privacy policy that contains a conspicuous link on the homepage; making users aware of the type of personal information that is collected and what it will be used for; listing all entities that collect students' personal information; and information on parental rights, which includes the right to refuse to disclose personal information or ask for a review and/or deletion of collected data [23]. Entities that collect data should also give direct notice before they start collecting data and seek and obtain verifiable consent before they collect or share/disclose the data.

GDPR

Within the education context, academic institutions collect considerable amounts of students' personal data, which also includes data from a special category that needs extra protection. Equally importantly, Mutimukwe et al. [24] reported that such personal data is also shared with third parties, many of whom are located in other countries. Thus, the GDPR introduced a series of changes in laws that relate to data protection across the world. Mutimukwe et al. [24] explained that the GDPR regulates how academic institutions collect, process, retain, and share personal data and that it also requires the institutions to have policies and structures to document the way they comply with the law. While the GDPR does not stop academic institutions from delivering education or administering exams, it requires them to be mindful of how they collect and store not only their students' personal and sensitive data but also data on their family members, school employees, and faculty [24].

Compliance with GDPR has to be demonstrated by documenting the steps taken during lawful processing of data, which means that schools must show how their processing of data is aligned with GDPR [6] [23] [24]. More importantly, the law may require a privacy impact valuation for new online proctoring tool, whereby the results of the valuation need to be considered during the development stages to ensure that data processing is kept to the minimum of what is required, a concept described by Mutimukwe et al. [24] as privacy by design. This means that GDPR outlines the requirements for data controllers and website operators to limit the processing of personal data to what is strictly necessary and for a very specific purpose. For institutions of higher education, GDPR establishes a set of lawful bases upon which students; personal data can be processed. Weiner and Hurtz [23] described the lawful bases as the acceptable circumstances under which data can be gathered and processed lawfully. These

circumstances include consent, legal obligation, performance contract, legitimate interest, protection of vital interests, and the exercise of official authority [24]. Without at least one the above circumstances, an institution may be found liable for unlawfully collecting and processing students' personal data.

In order to be compliant with GDPR, the law requires schools to identify the correct lawful purpose of collecting and processing student data. It also requires them to identify an additional lawful purpose for collecting and processing special category data [6]. Although consent is necessary for some institutions, Ziede [6] notes that GDPR requires care to be taken when such consent is relied upon as the basis for processing sensitive personal data and particularly special category data. The reason is that individuals retain the right to withdraw such consent at any time, denying the institutions the ability to process their data; however, withdrawing consent could also prevent the schools from availing the education services to the students, which is essentially a contractual breach of the school's obligation to the students and their parents [6].

Criticism of Current Laws

Although there are laws covering students' privacy, some of them have also been criticized for their inadequacy. FERPA, for example, only regulates the way academic institutions, school districts, and state education departments disclose students' data but do not regulate vendors and private companies directly to be bound by students' data privacy agreements [9]. As it has been found, students lost their constitutionally guaranteed right to privacy protections when the Department of Education gave companies that are not regulated by FERPA the permission to access students' information. (COPPA) was enacted in 1998 to specifically address children's privacy rights. However, studies [5] [18] [19] show that it does

not cover the wide scope of the modern privacy issues of students. Although COPPA obligates website operators to protect the privacy of children aged below 13 years, it is not tailored to protect students' data within the academic setting. Additionally, the FTC, which is the enforcement body, has also been criticized for failing to take strong enough measures to enforce the requirements of COPPA. Yet, when COPPA was enacted, FTC was granted powers by Congress beyond ensuring compliance with consent and notice regimes; it was given powers to demand the enforcement of limitations on website operators' ability to obtain, use, and store children's information [5].

FERPA has been described as a federal law designed to safeguard students' privacy and also gives parents and eligible students the right to access their data and control who can access it. COPPA was designed to protect the online privacy of children below the age of 13, whereby parents are required to give consent before their children's personal data is collected. It has been noted that while the law is not directly related to the education system, it emphasizes the need for protecting children's right to data privacy. GDRP was developed for the European Union and has been described as the most comprehensive data privacy law so far [24]. However, it is also worth noting that applying and enforcing these privacy laws in the educational setting and particularly to lockdown browsers is complex. According to Ziede [6], Weiner and Hurtz [23] and Mutimukwe et al. [24], academic institutions are encountering challenges as they try to balance the need for academic integrity with students' right to privacy and compliance with data privacy laws.

Strategies and Recommendations to Mitigate Privacy Concerns of Lockdown Browsers

As noted in this research, ensuring academic integrity in online exams while preserving user data privacy is a delicate balance. This dissertation proposes a technical solution that employs a combination of hardware and software elements to address common cheating methods and alleviate privacy concerns. By leveraging dual cameras, voice authentication, and local processing, the technical solution that will be proposed in this section intends to enhance the effectiveness of such remote proctoring tools as Respondus, ProctorU, Proctorio, and Examity, while minimizing the risk of data breaches and privacy invasion.

Hardware Configuration

Some of the cheating methods that institutions of higher learning are concerned with include use of unauthorized devices, books, or notes during exams [2]. To curb this, this research proposes a solution that incorporates two cameras, an inbuilt front-facing camera for facial recognition and voice authentication and an additional strategically placed camera to monitor only the student's desk area. This second camera can focus on the hands, keyboard, mouse, and screen, providing a comprehensive view to ensure academic integrity. As earlier discussed in this research, students were concerned that the camera settings of such tools as Respondus, ProctorU, Proctorio, and Examity were configured to record the entire room that the exams were taking place, thus raising privacy concerns [18] [44].

Authentication and Privacy

Voice authentication serves as an initial layer of security. The front-facing camera can be used to capture students' facial features and voice and verify their identity prior to starting the

exam. The online proctoring tools discussed in this research collect sensitive biometric data to confirm the identity of students prior to starting exams, which has raised a number of privacy concerns [46]. The proposed solution only captures a student's facial features and voice to ensure that the right student is taking the test while minimizing the collection of sensitive biometric data. The use of voice authentication also aligns with privacy regulations and emphasizes the importance of obtaining explicit consent [7].

WebRTC and Local Processing

To address concerns about data storage and usage, the solution will incorporate WebRTC, which enables direct communication between student devices and institutions servers. Despite the known vulnerabilities of WebRTC, it can be harnessed for its capability to establish secure peer-to-peer connections, which will ensure that the data is transmitted directly without intermediaries [48].

Local processing on students' devices is a pivotal element to minimize raw data transmission. This will ensure that basic image and audio processing, including facial recognition and voice analysis, are conducted locally. Such a solution can significantly reduce the amount of data transmitted and ensure that only relevant information, e.g., authentication results, is sent to the institutions' servers. This not only improves privacy concerns, but it also mitigates the risk of data breaches during transmission.

Addressing Cheating Methods

Screen Monitoring: The student's screen is captured by the front-facing camera, addressing the possibility of having additional browsers open for cheating.

Hand and Desk Monitoring: The strategically placed camera focuses on the student's hands, keyboard, mouse, and screen. It prevents the use of traditional devices, books, or notes during the exam.

Voice and Audio Monitoring: The voice authentication features will ensure that the students' voice is recognized and processed. Furthermore, audio from the room provides insights into any external communication or the presence of others, addressing concerns related to voice-activated devices, friends, or collaborations in the room.

Solution Requirements

The solution meets the needs of a remote proctor by providing a holistic view of the exam environment:

- **Student's Screen**: Captured by the front-facing camera.
- **Student's Hands**: Monitored by the strategically placed camera.
- **Student's Face**: Captured by the front-facing camera for authentication.
- **Audio in the Room**: Captured for voice authentication and detecting any unauthorized presence.

Discussion

As indicated in this research, due to the swift shift to remote learning brought about by the Covid-19 pandemic, many educational institutions and instructors faced challenges in adapting their courses for remote content delivery and exam proctoring. Course materials and assessments originally designed for in-person settings suddenly had to be administered and supervised online, prompting institutions to seek solutions for maintaining the integrity of online exams. While students acknowledged the challenges that their educational institutions face in

upholding safety measures, while continuing to deliver rigorous academic content at such periods like the Covid-19 pandemic, this understanding has not been beyond the end of the pandemic. This implies that while such times as the Covid-19 shows the people are willing to sacrifice some degree of personal privacy so as to adhere to safety protocols, such willingness seems to be hardly tolerated in a post-pandemic setting. From the content analysis, it was noted that a substantial percentage of students expressed substantial concerns, such as sharing personal information with proctoring companies, the extent of data collection, and the installation of proctoring software on their devices. Taken together, these insights indicate that many students perceived proctored exams as intrusive regarding their privacy and would prefer alternative assessment methods.

The analysis also revealed that a consensus exists among users regarding the importance of deterring cheating during exams. However, there is a tipping point beyond which users perceive monitoring as unnecessary and invasive. The monitoring elements that students found most unnecessary—such as tracking mouse and eye movement or web browser history—overlapped with those they found most uncomfortable and invasive. The content analysis revealed the users expressed discomfort with the monitoring of their eye movement, web browser history, microphone, and webcam. These are the same types of monitoring mentioned by students when they described how online proctored exams generated stress, feelings of being watched, and anxiety about minor actions potentially being flagged as cheating. These additional stressors and anxieties were reported to be distracting, reducing focus, and hindering optimal performance. The research suggests that, despite the availability of technologically advanced invigilation methods like 360-degree room scans and eye movement tracking, their necessity for preventing cheating is not evident, and they encroach on students'

personal privacy and device security. Implementing monitoring techniques that students view as unnecessary for ensuring exam integrity, while simultaneously requiring students to compromise their personal privacy, can erode trust in students and undermine their confidence in educators and institutions.