Andrea Franchini, February 2021

Do online proctoring tools ensure students' privacy and fair-treatment?

Abstract
This paper analyzes issues found in online proctoring tools (OPT), addressing in particular privacy and fairness concerns about this kind of software. While OPT are a solution that allows institutions to hold exams during pandemics, the way they work represents an invasion of students' privacy, raising the question of whether said invasion is justified in the name of academic integrity.
The lack of external regulation about OPT use of artificial intelligence (AI) results sometimes in biased systems that can discriminate students.
OPT that enforce strict requirements may also put at disadvantage certain individuals.

Introduction
Online proctoring tools (OPT) are a category of software that allow students to take exams remotely under strict supervision provided by a software, a human, or both.
While OPT have been around for more than a decade, the sudden shift to remote learning caused by the COVID-19 pandemic produced a surge in adoptions of such kind of software.
OPT allow institutions to hold exams sessions while preventing students from cheating (e.g.: using hidden notes, communicating with others or even having another person taking the exam in their place).

Because of their sudden and widespread adoption, there has been little time for institutions, and people in general, to address concerns about privacy and fairness offered by these tools, especially when deployed at such massive scale.

I believe that there is need for stricter regulations about OPT, as privacy and fairness play have a key role in this kind of software. This topic is crucial since we do not know how long this software will be adopted by institutions and the side effects they might have in the near-future. Major control over this technology can help avoid unpleasant situations for students.

With "privacy" I mean the fundamental right of students to have the bounds of their personal space respected by others. In a normal scenario, an institution should not have access or be interested in details of a student's personal life, beside the personal data needed for bureaucratic and administrative reasons. Whenever institutions overstep this initially set bound of their relations with students, we shall evaluate if it is necessary, and why.

In an education environment, "fairness" goes two ways.
The first is the students' relationship towards their instructors, meaning that students have to pledge to the institution code of conduct (e.g.: not to cheat during exams or engage in other forms of dishonesty). We may call this "academic integrity".
The other is an institution relationship towards its students, in which the first must guarantee inclusiveness, prevent discriminations of any kind from happening and ensure impartiality in evaluations of students' work. For example, exams should be accessible to all student regardless of ethnicity and gender, and account for students with disabilities.

Of course, privacy and fairness are related: when respecting the privacy of students, instructors may be more impartial during grading because they lack knowledge of private details that might make them biased towards certain students.

Better understanding of OPT can help both students and institutions in highlighting and addressing typical concerns of this technology; in particular, students should be better informed of how OPT work, and how these tools may represent a risk for their privacy and fair-treatment.

In this paper, I will try to offer compelling arguments on how students' right to privacy is often violated and how fairness is not always ensured when employing OPT.

How OPT and Remote Exams work

Before introducing my arguments, I want to better explain what an OPT consists of and how a remote exam works.

An OPT is composed roughly of two macro-components: the student's one and the institution's.
The first consists of a software run by the student's computer under the form of a web browser extension or application for the operative system. This software accesses the webcam and microphone connected to the student's computer, in order to record their behaviors during exams; it may also require students to share what they see on the screen with their instructors.
In certain cases, it can also prevent the student from using other softwares unless explicitly allowed.
The latter is used to process and store said recording of students, showing them to instructors during or after an exam, and flag suspect behaviors of students.

The most well-known and diffused OPT are commercial proprietary software that is licensed to institutions. Most OPT companies also provide hosting solutions for institutions, meaning that recordings are stored on the company servers instead of the institution servers.

A remote exam requires students to authenticate themselves in order to prove their identity, usually by framing a valid document, and to scan their room, to show that nobody else is present and that they do not have any unapproved material.
Once the exam starts, students need to remain framed by the webcam for its whole duration, and suspect behaviors such staring in another direction or people talking are notified to both the student and the proctor (human or virtual). This analysis is usually automated and carried out by an artificial intelligence (AI).
Students also must not interact with any other computer application if the latter is not already blocked by the proctoring software.
Depending on the configuration, an OPT may require a review by a human proctor before disqualifying a student when enough reports of suspect behavior are present.

Privacy

The first privacy issue with OPT is that such tools require students to record not only themselves, but also their entire room. This causes OPT to collect a huge quantity of data that are related to the student, but ultimately unrelated to the exam. Some services such as ProctorExam even require the use of a smartphone as an additional point of view to record the back of the student, therefore obtaining a detailed, 360-degrees view of the room. In addition, there is a chance to expose personal details of a student private life when they are required to scan their rooms in the authentication process. Some students may agree with such methods, but others may not want to be forced to expose personal spaces to an external eye, especially when they must share a room with others during lockdowns caused by a pandemic. Because the perception of what is private is often subjective, it is difficult to make absolute conclusions about it.

In my opinion a full scan of the room is an invasion of the students' privacy from an ethical point of view for the following reasons. In a traditional exam held in a classroom or similar facility, students can see who is watching over them, and beside their physical person, no other personal information is directly deducible. In a remote exam context, though, the overseer is no longer in students' reach: it becomes an abstract entity that do not directly interact with them; it may also not be their instructor, but an employee of an OPT company.

Let's make the hypothesis that in an exam held in the classroom the privacy of both students and their proctors is respected: both sides have few ways to violate each other privacy, and if they did, it would be immediately witnessed by others.
In a remote setting students cannot know who, if any, is watching their recording, and what are they looking for. Often, students do not even have access to their own recordings,

because they are managed by the institution on their behalf.
Thus, the access to private information on each side is no longer symmetric, and students have more to lose in a remote exam than in a classroom exam. Students need to sacrifice their right to privacy to be able to take exams: if no alternatives are offered, though, it is very likely that students would rather take an exam with a tool they do not agree on, rather than forfeiting it, putting them in a difficult position. The idea of having a stranger peeking in one's room is often unsettling for some people, and students are even more legitimated to be wary of such tools when many universities decided to have mandatory proctored exams by using OPT. Of course, this led to widespread protests from students (Kelley 2020).

A possible counter-argument by supporters of OPT is that since students already have to allow an invasion of their privacy in the classroom, by being closely monitored by instructors, remote surveillance is ethically equivalent in-classroom surveillance. An excellent confutation is provided by (Coghlan, Miller, and Paterson 2020), who state that to make in-classroom exams truly equivalent to remote ones, there should be a proctor in front of each student staring at them for the whole duration of their exam, possibly with an AI assistant to analyze each minuscule face movement.
I find this last argument plausible because it shows that remote surveillance, thanks to the presence of AI tools, allows instructors to monitor students in greater detail, and that such strict surveillance if actually carried out in-class would be definitely unsettling to a student. In addition, OPT allow a single instructor to monitor many student at greater detail, a feat that would be unrealistic in a traditional classroom, further proving the non-equivalence between remote and in-class proctoring.

I believe that OPT and institutions should address with more consideration students that desire a higher level of privacy. Let us consider the following example: student A wants to share the least amount of private details with the proctor, while student B does not care. If we regard mostly B's view, possibly requiring them to share a detailed recording of their room, then A has more to lose than B, namely B's privacy. If we consider the opposite case, though, since B does not care, A is in a better position. Thus, in this kind of situations, it is a better compromise to second B's needs.
We might also want to examine a possible reason for B lack of interest: perhaps B was not informed in a direct way of what are the implication of the use of OPT. While OPT clearly explain to students which of their data they will have access to, but how these data will be processed in detail is not specified.
While this example seems to work, we are not considering an important factor, which is the role of the proctor (human or virtual). To prevent cheating, institutions employ OPT to make sure that cheating material and other people are not present.
First, the system receives the integral audio and video recording of students and stores them, then analyzes them to determine whether there was an instance of cheating.
It is obvious that OPT end up with lots of irrelevant data for their purpose, such as a picture a student may have on their wall, or how big is their house. Then why and for how long these private data should be stored when they no longer serve a purpose?

An immediate answer would probably state to discard them immediately, as they no longer serve a purpose.
There is actually little reason for a proctoring tool company to actively discard such data that is embedded in a video recording, as it would mean to actively dedicate resources to edit out the details, for example by blurring them.
To a machine trained to recognize objects like smartphones, since it is not a sentient being, it should not really matter who the subject of a photo hanging from the wall is (except in cases where bias is involved which I will analyze in the next section). It also should not affect the security of students unless a malicious design is involved.
With a human proctor, the situation is a different: there is no technologic protection put in place to make sure that a proctor does not focus too much on details that are already deemed unnecessary. Most importantly, they

must not disclose or use for other purposes those recordings without consent, for example, by taking a picture or a video with their smartphones and sharing it online. Should that happen, that would result in a massive violation of a student's privacy.

In addition, companies often reserve their right to retain recording for long period of time, for a maximum of five years in the case of Respondus and two years in the case of ProctorU, or they delegate this right to institutions, as ProctorExam does: in both cases, it is out of students' control whenever this data is deleted or accessed.

A question that we must ask ourselves is whether such invasion of privacy is justified in name of the academic integrity.

While the interest of institution in preventing cheating is clearly legitimate from an academic point of view, and it is already enforced during in-class exams, the way OPT have been quickly adopted makes me think that these tools have been seen as an easy solution to the complex problem that is remote teaching. I said "easy solution" because OPT have been developed with one and only one purpose, that is to detect students that cheat. Other "more complex" solutions, such as rethinking the structure of an exam to make cheating harder, clearly require effort from the instructors and therefore this option usually is not immediately considered as an alternative.

Fairness

One critical issue is the perceived fairness of OPT. My argument is that due to their unclear inner workings, it's hard to prove that OPT are truly fair and unbiased in their job and use.

The first immediate consideration about OPT is how little we know about how they function internally.
I will argue that it is not possible to prove the fairness of OPT if we cannot trust them first. This is caused by two factors: the use of AI, and the proprietary license of these tools.

I'll address first the proprietary nature of this kind of softwares. Since OPT are commercial products, it is in their owners' interest to prevent their competitors from learning how their software works, therefore their source code is often kept secret. In addition, OPT companies usually offer their product as a service, meaning that the software runs on their servers and the data is usually stored in a datacenter under their control. This means that an external party has no way to know how an online proctoring system works: it is in fact a blackbox to them.

In my opinion, OPT being blackboxes represent a major concern about the trust we put into these systems. Although companies must respect strict requirements about how they must handle their customers' data, security breaches are possible, as in the case of ProctorU (Abrams 2020), and represent a threat to the students' privacy and the trust that student are required to put in these companies.
I believe that if these companies open-sourced at least parts of their code, there would be a great benefit for all: third-party analysis may highlight flaws that a company didn't notice, concerned users might have the possibility to better understand how the software works and companies would still be able to monetize their product through licenses and by providing the service just as they already do.
I think that (Hoepman and Jacobs 2007) offer a detailed analysis on why open source is not a liability for companies that handle sensible data, showing that it's more convenient to trust a company that opens its software and design to a public inspection than one that keep the inner workings secret.
This could help build trust between students and proctoring tools, and, most importantly, allow institutions to make a more informed choice about which OPT to adopt.

The other reason why it is hard to understand how an OPT works is the use of AI.
With the advent of machine learning, most AI are trained on huge datasets, which makes them harder to replicate and to understand.

Since AI are great at repeating complex task in a shorter time than humans, they are used in OPT for two purposed: speed up authentication, and identify suspect behaviors. On paper, AI should do their job without issues but in reality, they have many edge cases in which they fail. Yet, because of their complex nature, it is hard for a company to pinpoint the issue, and even harder for an external viewer to figure out why the tool is not manifesting the correct behavior.

When an AI fails to do its job, or does it wrong, there are serious implications. It is also important to understand what is behind a misbehaving AI.

One common issue with AI used to analyze images of humans is that they often fail to recognize certain individuals.
This is often the result, in the best scenario, of an oversight from the AI designers and in the worst, of an intentional malicious design: in both cases, the result is a biased AI, that often produce racist or sexist outputs. For example, people of color have trouble being recognized by such systems, that either think that no person is present, or that there's a lack of light. Another example is how a rigid classification into "male" or "female" that simplify the development of an AI fails to properly categorize transgender and non-binary people (Gebru 2019).

In a OPT authentication process, a student ID is compared to what the webcam is recording, usually to prevent someone else to impersonate a student. If a webcam isn't able to detect a face, or the algorithm thinks that the person visible to the webcam does not match the student ID details, it may deny them the possibility of taking an exam, or require the intervention of a human proctor.
My belief is that such a strict system is unfair toward students for the following reason. The only advantage of an automated process is a faster admission to an exam for many, possibly white, gender-conforming students, at the expenses of a minorities that need assistance because of faulty software. This is not an acceptable compromise for any institution that values the equal-treatment of their students, because if the software consistently misbehaves in presence of certain individuals, it clearly does not ensures that the latter are treated fairly.

Another drawback is that students forced to require assistance may also go through embarrassing and possibly traumatic moments: for example, a transgender student may be outed by the system to a stranger, and they need to be notified of the possibility of such situations (Swauger 2020).
These cons lead me to think that AI-based authentication systems are largely unnecessary because they try to make the manual authentication of students a problem, when it was not in first place: instructors could verify identity of students manually in a similar fashion to what happens in a in-class exam, or, if the time is a concern, during the exam. It is unclear to me, though, why a company would push for the use of AI for authentication as a solution.

There are still issues that happen during an exam. The first one is how OPT present a classist view in how they expect a student to setup their workspace in preparation to an exam, the second one is what should an OPT see as a presence of misconduct.

OPT, as already said, require students to setup their workspace adequately, meaning that the ambient should be well lit, without noise, people, pets and that they should be visible, possibly from two angles. My argument is that the requirement of OPT are not fair towards certain category of students.
Especially during lockdowns, students who live in a one-room flat with their own family may not be able to find sufficient space to satisfy the OPT demands. It may be impossible for a student whose parents work from home and have little siblings to find the necessary space and quiet in order to take an exam: it is likely that someone else will end up recorded by the webcam. Beside the student, this kind of situation creates uneasy conditions for others: for example, students living with toddlers can not be sure that there will be silence during their exams.

Since OPT require an Internet connection with a fair amount of bandwidth, this might hinder tasks like remote working, not be a reality in first place, especially for students living in remote areas.
Comparing this scenario to one in which students have their own room, OPT favors the latter, thus treating the first unfairly.
Noisy neighbors might also be a problem, as not all houses have a good sound insulation and load voices may be flagged by system.
I believe that institutions that do not allow alternative methods or provide students with a public space with all due safety precautions where to take exams are unfair in the treatment of their students, in this case with proctoring tools representing as a gap between students who can afford better conditions (a larger place, stable Internet connections) and those who cannot.
Similar concerns are raised by (Coghlan, Miller, and Paterson 2020), who also propose that universities might loan devices for students who cannot afford a computer or webcam, as well as allowing selected student to take their exams on campus. They highlight how this solution might cause delays in courses and other logistical issues. While I agree with such solutions, I believe that offering students alternatives in these kind of situations should be a priority for any institute.

During exams, OPT analyze student behaviors in search of possible sign of cheating. I believe it is quite hard to make an arbitrary list of what is cheating and what is not. Therefore, designers of OPT have tried to guess what is a likable sign of cheating. Turning the head, averting the gaze from the computer screen, but also scratching and other minor movements are sufficient to get a student behavior flagged as suspicious.
In my opinion watching out for such a huge number of factors is excessive, especially in light of evidence that not always a directional change of a student's gaze represents an instance of cheating; nonetheless many behaviors that can flag a student are also signs of anxiety (Kolski and Weible 2019).
This creates unfavorable conditions for students that have disabilities or more generally have involuntary behaviors caused by anxiety or tics.
I believe that systems that are too strict, notify students too much or even stop their exams for some seconds in presence of suspicious behaviors can negatively impact students' performances an produce an unnecessary uncomfortable experience.
Even for neurotypical, able-bodied students it is natural to stretch, roll up eyes in front of a difficult question, or softly re-read their answers to relieve stress, yet such behaviors are supposed to be a sign of cheating.

Being flagged repeatedly may cause a termination of a student exam, in certain cases. To prevent this kind of situations, the decision of what to do with flagged students falls to a human proctor, when present. At first we might think that the presence of a proctor would make a system less biased, but it in reality people can over-trust AI or may be unsure on how to interpret the findings presented to them by the AI (Coghlan, Miller, and Paterson 2020).
I believe that the claim of human proctors not being completely reliable is plausible, because a proctor who isn't familiar with the student might not be aware of a student possible conditions. An instructor that sees a student repeatedly flagged may also want to question them separately to assert their effective knowledge of the exam's subject: while it is the instructor's job, it may be unfair for a student whose behavior would have otherwise gone unnoticed in class, thus causing unnecessary stress.

I want now to discuss if it is possible to ensure fairness in OPT.
I believe that in their current form OPT are more of a trouble to students than an helpful tool. They represent a vision of technology as barrier to illicit behaviors such as cheating, rather than an enabler of new way of teaching and assessing students' abilities.
While a poorly designed AI might be eventually fixed, I believe that its use can still raise concerns because of the difficulty in understanding such tools, thus the need of stricter regulations pertaining the use of AI with personal data.

The idea of preventing cheating is clearly motivated by the will of institutions in ensuring a fair exam to students, and I agree with such view, but extra care needs to be taken to ensure that the exam is fair towards students with disabilities or who are neurodivergent.

Conclusions

While OPT represented an immediate and easy solution for institutions looking for a way to hold exams during a pandemic, few concerns have been raised about the use of such technology, in particular about privacy and fairness.
These tools invade the students' privacy and collect huge amount of unnecessary data, a far greater amount than what could be gathered from an equivalent, in-class scenario. The way recording of students are stored and accessed also raise concern regarding their illegitimate use.
Fairness has to be ensured when the design of such tool requires the use of AI to process recording of students, in order to prevent discrimination and false positive caused by students that have disabilities or are neurodivergent.
Today, these tools are common despite the lack of strict and specific regulations about their use, which are needed to better safeguard students' privacy and rights to a fair education. Institutions should take additional care in deciding whether to use these tools, inform students in detail about how these tools work, and to opportunely configure them in order to allow student major control over their data.

Bibliography

Abrams, Lawrence. 2020. “ProctorU Confirms Data Breach after Database Leaked Online.” BleepingComputer. August 9, 2020. https://www.bleepingcomputer.com/news/security/proctoru-confirms-data-breach-after-database-leaked-online/.

Coghlan, Simon, Tim Miller, and Jeannie Paterson. 2020. “Good Proctor Or "Big Brother"? AI Ethics and Online Exam Supervision Technologies.” ArXiv Preprint ArXiv:2011.07647.

Gebru, Timnit. 2019. “Oxford Handbook on AI Ethics Book Chapter on Race and Gender.” ArXiv Preprint ArXiv:1908.06165.

Hoepman, Jaap-Henk, and Bart Jacobs. 2007. “Increased Security through Open Source.” Communications of the ACM 50 (1): 79–83. https://doi.org/10.1145/1188913.1188921.

Kelley, Jason. 2020. “Students Are Pushing Back against Proctoring Surveillance Apps.” Electronic Frontier Foundation. September 25, 2020. https://www.eff.org/deeplinks/2020/09/students-are-pushing-back-against-proctoring-surveillance-apps.

Kolski, Tammi, and Jennifer Weible. 2018. “Examining the Relationship between Student Test Anxiety and Webcam Based Exam Proctoring.” Online Journal of Distance Learning Administration 21.

ProctorExam. Last accessed Feb 2021. https://proctorexam.com/.

ProctorU. Last accessed Feb 2021. https://www.proctoru.com/.

Respondus. Last accessed Feb 2021. https://web.respondus.com.

Swauger, Shea. 2020. “Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education.” In Critical Digital Pedagogy. Pressbook. https://cdpcollection.pressbooks.com/chapter/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/.