Transcript for EdTech Sandbox Series: Remote Proctoring Through an Ethical Lens: The Case Against Surveillance
BCcampus Panel Discussion hosted on October 17, 2025
Host: Gwen Nguyen
Facilitator: Ian Linkletter

IAN LINKLETTER:
My name is Ian Linkletter. I'm an emerging technology and open education librarian at the British Columbia Institute of Technology. My presentation today is called Remote Proctoring Through an Ethical Lens, and all of my slides and links are available online at bit.ly/againstproctoring I'd like to acknowledge that I live and work on the traditional ancestral, and unceded territory of the Coast Salish Nations of Squamish, Tsleil-Waututh, and Musqueam. As I reflect on 20 years this year since I immigrated to Canada, I acknowledge that I'm part of a long history of settlement in a country that attempted cultural genocide through the residential schools program as recently as 1996. I'm grateful for the knowledge that I have gained and commit to do more learning, more teaching, more acting through the Truth and Reconciliation Calls to Action.

An overview of the session. This is sort of how it breaks down. I'm going to have a 30-minute presentation right now making the case against remote proctoring. We're going to have three, 10-minute case study conversations. Don't worry. No breakout rooms. Stick around. It's going to be a fantastic conversation, and it's going to be framed around the question, what would you say in certain situations? I'll go back to my slide deck again to talk about algorithmic impact assessments, which are a way to protect students from the harms of AI, and were recently implemented at BCIT. Then we'll have a wrap-up discussion with any loose ends, unexplored thoughts, or additional questions for me. One more time, my slides and links are at bit.ly/againstproctoring.

I was really fascinated to learn from Gwen and Britt the results of the participant survey for this session. So we had a lot of registrants, and this is how they broke down when we asked what role that they have, what role you have. So we had about 6.5% administrators, and this made me really excited. 31.5% educational developers, instructional designers, faculty developers, and learning designers. This is fantastic. I myself am not a learning designer. And when we talk about academic integrity and how to design assessment to secure, to be as effective as possible, learning designers are such a key part of that situation and scenario. We have educational technologists, web developers, librarians, staff, not so many students, but maybe next time, I hope. And we have a lot of faculty, sessional instructors, teaching assistants, and instructors. We have 29.6% faculty. So that's really exciting. The combination between learning designers, ed techs, faculty, librarians, staff, it's the combination that needs to be in the room. A bit about myself and my background.

I'm a graduate of the Evergreen State College in Olympia, Washington. Evergreen is constantly targeted by Fox News because of its graduates and alumni and faculty that are dedicated to social justice. The University of Western Ontario was where I got my master's in Library and Information Science, and for 14 years, I was a practising educational technologist, working at Fanshawe College, BCIT, and UBC. I spent 10 of those years at UBC's Faculty of Education, where I learned so much from the faculty that I worked with about ethical educational technology. I've been with BCIT Library since 2022. In 2024, I created the Canadian Privacy Library, accessible at privacylibrary.ca, which contains over 500 privacy impact assessments from most of the B.C. public post-secondaries. Recently, I joined Brock University's Inclusive Education Research Lab, led by Dr. Rajiv Jhangiani, where I'll be working on student-led research into the ethical educational technology policies at Canada's largest universities. "Do no harm" is my fundamental principle, and I think makes me quite unique. I think about technology and the use of ethical educational technology. I always think about scale, and I've learned over time that if one student is reporting an issue or a problem or harm, there are many, many more that are experiencing the same thing and don't reach out. So doing no harm is my way to make sure that we are protecting all students, one student at a time.

My fight against academic surveillance is something that many people know about. It has made national, international news since 2020. So let me describe the situation in my own words. In 2020, I worked in UBC's Faculty of Education as a learning technology specialist. And when we shifted to emergency remote teaching in 2020, proctoring boomed, over 50,000 UBC students were forced to use Proctorio, an AI proctoring system. And I was paying attention to what they were saying online. Through Reddit, through Twitter, through social media, students were expressing that they were very upset at being forced to use the technology. They considered it an invasion of privacy, rightfully so, and were just felt horrible that their institution that they loved and trusted was forcing them to do this. Was also paying attention to the CEO of Proctorio's behaviour because he was actually going into the UBC sub Reddit and Twitter and so on to target students that criticized the product online. I defended them and that got me on Proctorio's radar. In August of 2020, I found help videos on YouTube proving that the technology was harmful by showing its inner workings, and I shared my concerns citing the YouTube links as proof. On September 2, 2020, I was sued for copyright infringement. The allegation is that by sharing YouTube links, which were unlisted, I was actually committing copyright infringement and breach of confidence, which obviously is not true, and parts of the lawsuit have already been thrown out of court. But the good news is that in March 2021, six months after the lawsuit was filed, UBC banned Proctorio with slim exceptions. The lawsuit continues to this day, unbelievably, over five years later, but I will never be defeated. I will never give up. I will never stop caring about students and doing everything that I can. This lawsuit has no effect on my advocacy. I'll be talking about Proctorio in this presentation, and I'm not afraid. You can learn more and follow my journey at linkletter.org.

So what is academic surveillance software anyway? On screen, I have an image of one of those giant ghosts from the video game Super Mario World. This is kind of my villainous analogy for

the academic surveillance software industry. Academic surveillance software polices student behaviour, and it's not EdTech. This is a very important differentiation. Right now, academic surveillance technology is eating up our EdTech budgets, eating up our learning design budgets, our teaching and learning centre budgets, and that's just not appropriate. If an institute wants to spy on students, it should have a budget for that, and that should be transparent. Educational technology serves a pedagogical purpose, but surveillance technology actually has no place in education because it serves no pedagogical purpose. As community members, as faculty, as learning designers, as staff, we can work together against surveillance and find a better future.

Some examples of surveillance software, many of which come from the K through 12 system and many of which are more popular in the United States include screen monitoring software like GoGuardian, online activity and communication monitoring, like Gaggle. Gaggle has been in the news recently because they flag certain words like gay, and that can out students and subject them to unnecessary and unwelcome scrutiny and attention from instructors. Learning analytics. This is a little bit controversial because I know this is a lot of people's bread and butter, but learning analytics, which are often in the LMS, can be an example of surveillance, depending on how they're used. And quiz activity logging, like in the Canvas learning management system, is another example. So quiz activity logging shows what a student was looking at. Did they switch tabs? How long did they spend on a question? And quiz activity logging has controversially been used at institutes in the United States like Dartmouth Medical School, and then unused when the company itself in structure said that it wasn't appropriate to use as a sole measure of cheating or dishonesty. AI detection is another example. I could and have done presentations solely about AI detection. You can refer to my last year's presentation Beyond Surveillance for more information about why it's unethical to use. Turnitin is the big one. And lockdown browsers are another example. So Respondus Lockdown Browser is a key player. You can learn more about the harms of academic surveillance software from the Electronic Frontier Foundation at this link, which is on my document.

So surveillance really demonstrates values. It demonstrates that an instructor values power and control over teaching and learning. And I'll say that again, power and control over teaching and learning, because we know that forming a sense of community in a classroom with mutual trust between the instructor and the students is what contributes to a positive learning environment, and a classroom without mutual trust is not a good place to be. So if you can imagine being a student reading the syllabus on day number one, and it's talking about how you're going to be recorded and AI is going to analyze your behaviour, and proprietary algorithms will be used to determine whether you get an A or whether you fail the class. That's totally inappropriate and something that I think upsets students. It makes them feel creeped out. I've heard the phrase proctorio professor used before. It's not a reputation that you want to stick to you.

So I really recommend not using academic surveillance. It sends a message to students that you are not trusted, we are watching you and you can be removed. And that threat of removal is

really something that's quite profound because it can lead to the loss of scholarships, the loss of work visas, the loss of graduation opportunities. It can really have profound, resounding impacts through a student's life. So getting it right is necessary, and the false positives that are common in these tools is unacceptable.

There are various types of remote proctoring out there kind of on a spectrum. So from, you know, I was going to say least invasive to most invasive, but let's just say that these are all invasive. From the beginning, we have lockdown control, which as I mentioned, restricts switching apps or tabs. It also prevents copy-pasting, printing, and other actions. Then we have the live proctoring systems where a human typically in a call centre somewhere in the world watches a live video feed and can potentially interact and intervene. I've read stories of human proctors moving a student's mouse or talking to them or making distracting sounds, which is obviously not good. There's AI plus human remote proctoring tools, which use algorithms to monitor and flag certain behaviours, which are then reviewed by humans after the fact. And then finally, there's AI decision-making tools where an AI system controls access to the exam, calculates suspicion score for the instructor with no input from them, and it can unilaterally decide to remove students from an exam with no human oversight.

Common rationale for proctoring, kind of the reason that it existed to begin with prior to the pandemic and reasons that it's still justified today by people that maybe aren't familiar with all of the issues with it, are that it helps meet accreditation requirements. So certain fields like for example, lawyers in law school have to take proctored exams, and so that's one use for it. Of course, proctoring can also take place in person. Ensures exam integrity. So this is obviously not something that actually I keep saying the word obviously today. I'm going to pick a different word. This is not something that is actually guaranteed through the use of proctoring software. It's the goal. It's the objective. It's the marketing lingo. But I will point out that exam security is different from academic integrity, and people that are in the academic integrity business actually refer to exam security as separate from academic integrity with proctoring being something that feeds into exam security and does not ensure integrity, like many vendors will tell you. And also, maintaining credential value is another factor. During the pandemic, the CEO of Proctorio was referring to students currently in school as you don't want to get a Corona diploma, right, which was super offensive and actually the biggest attack on academic integrity that I saw during the entire pandemic.

Remote proctoring with AI is where I'm going to focus today because it's the most egregious and has the most ethical concerns with it. Proctorio, it's no surprise that Proctorio is the focus of my presentation today. I say that not because Proctorio is suing me and has tried to ruin my life, but because they are actually the worst of the worst. They fully automate decision making. They monitor students using AI. They rank students by suspicion level, they survey your webcam, browser, and microphone, and the room scan functionality, which they perpetuated was found to be unconstitutional in 2022. A student at Cleveland State University sued his school for unwarranted, unconstitutionally surveilling him inside the privacy of his own home,

inside the privacy of his own room, and a court found that that was unconstitutional and Cleveland State University had to stop. So this led to a lot of introspection from universities and institutions about whether room scans were appropriate. Companies like Proctorio, dodged this concern by renaming room scans to desk scans, but the concerns are still valid. You're spying on a student in their room, and that's not appropriate. On the left hand side, I have a synthetic image created with ChatGPT. ChatGPT image generation can be useful for creating screenshots or images that you won't get sued for sharing. So this is not a screenshot of Proctorio. This is a ChatGPT-generated image of a creepy instructor looking at a dashboard of different analytics and charts and graphs and a very close upshot of a student with a bull's eye in both of her eyes tracking where she's looking. A good analogy, I think.

Proctorio uses what it calls abnormalities, so called abnormalities with Drew Harwell at “The Washington Post" describing the system like this. "One system, Proctorio, uses gaze-detection, face-detection, and computer-monitoring software to flag students for any “abnormal" head movement, mouse movement, eye wandering, computer window resizing, tab opening, scrolling, clicking, typing, and copies and pastes. A student can be flagged for finishing the test too quickly or too slowly, clicking too much, or not enough."

And so this is really the root of why AI plus proctoring equals harm because this proprietary black box system discriminates against disabled students. It discriminates against students of colour, as I'll go into a lot. It's an unwarranted invasion of privacy, as that court found, and it causes emotional harm. Because imagine this. Imagine the webcam on your own computer betraying you in the privacy of your own home. What does that feel like to know that the AI is tracking your eye movements and flagging to your instructor every time that you looked away or coughed or, it's unconscionable. Oh, gosh, I don't know how to pronounce that. My apologies.

So proctoring is actually an accessibility barrier, and it blocks access if it cannot detect a face. It's actually a form of denying access. Inaccessible to blind students who may not be able to maneuver their computer and webcam in a 360 way. It kicks you out if you step away from your computer to use the bathroom or take medication. If it doesn't detect your face, it can kick you out. If it detects another face, like a child or somebody that you're responsible for taking care of, it'll just kick you out. No recourse on that. And the eye and head movement tracking specifically targets neurodiverse students who may move differently from normative students. So it's all very concerning, and minimizing movement is a very stressful experience.

Today, we're going to be looking at proctoring and considering proctoring through ethical lenses, and I wanted to draw attention to a recently published document by the Province of British Columbia and BCcampus and many well-respected educators in the province. It's called the B.C. Post-Secondary Ethical Educational Technology Toolkit, and I'll be reading through some of the lenses that it encourages us to consider when we procure and implement technology. So the toolkit provides guiding questions, resources, and tools for educators,

administrators, and staff in B.C post-secondary institutions to critically evaluate and adopt educational technologies. It outlines key considerations on a variety of topics, equipping users with a framework for ethical decision-making regarding educational technologies.

One of the lenses that it encourages you to look at technologies through is equity, diversity, and inclusion with two bullets from the report saying, “Considering inclusivity in educational technologies involves considering diverse backgrounds, contexts, and world views. An intersectional approach plays a key role in addressing the needs of various groups and includes analysis that considers how different aspects of a person's identity, such as race, gender, socioeconomic status, sexuality, disability, etc., intersect, overlap, and interact to influence a person's experience in the world. Inclusive decision making involves engaging the diverse identities, cultures, and perspectives within your institution's community in decisions related to educational technology, such as procurement, the adoption of new tools or policy development. Procurement is such an important part of these conversations because it's the earliest opportunity that we have to make sure that we're not accidentally procuring technology that's unethical without considering all the ramifications. I really honour the work of Anne Marie Scott and Brenna Clark Gray, who write about how procurement actually has institutions paying more attention to the origin of coffee cups and tea bags than the ethics behind things like surveillance software.

Understanding and addressing bias is another important factor. So reading a few points from the report, which is linked and in my notes, “Identifying and understanding potential biases that may be embedded within tools should be considered when implementing EdTech. The growing prevalence of AI technologies embedded within EdTech makes such risks more important to understand and consider. Examples of potential biases include algorithmic bias, which can occur when technologies produce results that reflect prejudices present in the data used to train them or when biases are introduced through design choices made during the development of digital tools. Various factors contribute to bias, including a lack of diverse perspectives during its development, bias in the datasets used for training, and deployment methods used, carefully weighing the risks and consequences associated with these biases helps to foster equitable outcomes for all users."

And I also want to draw attention to Brock University’s Ethical Framework for Educational Technologies, which was recently approved by its senate, and it reads that in the section about bias, it reads that “For educational technologies such as artificial intelligence applications that include automated functions, it is important to identify and consider algorithmic biases and to evaluate the risk not only to institutions and individuals, but also the risk to groups and communities like persons with disabilities, BIPOC educators and students. With awareness of the protected grounds of the Ontario Human Rights Code, this includes ensuring that the hidden value judgments that are racist, ableist, or otherwise discriminatory are not baked into educational technologies, and the example that they use for an avoidable risk is procuring a

remote exam proctoring tool that disproportionately flags students with darker skin tones as cheating.

Moving back to the ethical EdTech guide put together by the province, Indigenous intellectual property, information governance and data sovereignty is also mentioned with shoutout to the five Rs of Indigenous pedagogy, which include relationships, respect, relevance, responsibility, and reciprocity when using educational technology. While these five Rs are not universal to all Indigenous Peoples, they are something that has been researched and shared by the Faculty of Education at UBC, and you can learn more about them at the link. We have two more.

So advancing care, well-being, and community, “Integrating educational technologies in post-secondary institutions in a human-centred way that considers the physical, emotional, and psychological safety of learners, educators, and staff can help create a safe and supportive environment. This includes consideration of digital well-being and fostering supportive online communities. By considering inclusiveness, safety, and respect, EdTech can be used to help create an environment where people can thrive.

Then finally, environmental sustainability, which I won't talk about further in this presentation, but if you've seen other presentations by me, I am obsessed with this issue. The issue of environmental sustainability, bias, and all of the other issues with the use of artificial intelligence do apply to academic surveillance software, especially when it uses AI, but really any cloud-based technology should have you considering environmental impacts, including carbon footprint, energy consumption, and both physical and electronic waste. By assessing these technologies through the lenses of ecological, economic, and social sustainability, we can align technical advancements with environmental responsibility and stewardship. These are some lenses that we can consider, but I will really be focusing on bias because as Brock University said, it can actually lead to a violation of the Human Rights Code. It can actually be unlawful to use programs that we know are discriminatory.

Dr. Chris Gilliard is one of my favourite surveillance scholars online. He's been deeply influential to me, and he writes, "Imagine all you want to do is take a test, and the system your institution uses as a gateway to testing doesn't recognize you as a human being." This is actually the case.

I want to well, anytime that I talk about remote proctoring, I always want to honour and centre the student voices that are all around us. Robin Pocornie is a student or was a student in the Netherlands who had a horrifying experience being forced to use Proctorio by her school.

[VIDEO]
I sit behind my desk for my first exam of my new studies. It's a pandemic, so we're using online exam software that surveys students to check if they are cheating or not. We call this proctoring. I sit behind my desk, I login.

IAN: Sorry, I'm going to turn on the captions. My apologies.

[VIDEO]
My name, Robin Aisha Pocornie and my password. Welcome 123!. And it has a facial detection step. I sit in front of the camera and I wait for it to count and it counts one, two, three, smile. Takes a picture and it tells me, face not found, room too dark, which is interesting because it's broad daylight out and I'm in a well-lit room. I'll try again because we only get 15 minutes to log in and after these 15 minutes, we are barred from the exam. You have to log in on time and I sit there again and I sit one, two, three, smile. Again, it tells me, face not found, room too dark. In the darkest of times, we must create light. That's what I do. I grab a lamp and I just shine it bright in my face and I one, two, three, smile and bam, it works. I get into my exam. After the exam, I go on the student discard channel. This is basically a forum where we talk about our experiences as students. On there, a lot of students are explaining that this software doesn't work for them. They hate it, it's very invasive, but none of them are talking about what I've experienced. Face not found, room too dark.
[VIDEO ENDS]

IAN:
So Robin is a very inspiring student. I have some more to say about Robin and her experience. So after not being supported, Robin filed a complaint with the Dutch Institute for Human Rights. Hans de Zwart and Naomi Appleman of the Racism and Technology Center supported her journey, helping vouch for her credibility with journalists and offer her legal support. Robin is also a member of the Racism and Technology Center, which has a website at racism ndtechnology.center where you can learn more about Robin's case. The case set human rights precedent because for the first time in history, it was affirmed that technology itself can be racist. Her complaint about the technology not seeing her face was seen as an example of the potential for technology itself to be racist. So regardless of the intent of the developer or the instructor, just using a technology, even unknowingly that has a racially biased outcome is a racist practice. Ultimately, the institute concluded that it didn't work because of her glasses, not her skin colour, which was obviously a huge disappointment and something that I'll go back to later because maybe there's more to the story research shows. The Institute also found, though, that VU, her university, had discriminated against her by not taking her seriously.

I'd like to watch one more video with you. It's about 1 minute and 30 seconds. My thanks to Mozilla for licensing at CC-BY-NC on YouTube, BCcampus.

[VIDEO STARTS]
Back in February, I had to take a test. It was a lab quiz for my biology class. Thank you. You took it remotely due to the pandemic. I'd woken up in my dorm room that day, sat down, and now I was ready to take my test. The lab quiz required me to use software I'd never seen before. Prior to taking the actual quiz, I wanted to use the practice quiz. It did not go okay. The software we were using couldn't see me, and I had tried everything. Shades down, lights on. I had my lights

off and my shades up, half my lights on, half my lights off, shades down, shades up. I tried everything. None of this made sense to me. It was noon, so I knew there was a lot of sunlight in my room. Eventually, what worked was me standing in the middle of my room, my lights on, my window shade down, directly under the light. I didn't really want to take my quiz standing up under a light. I got an idea. My dad had gifted me and my sister some LED grade construction flashlights. So I had a thought. What if I put my lights on, my shade down facing south and using the flashlight pointed at my face directly? That's what worked. It had taken me 45 minutes to get the app to see me properly. The quiz itself was only 30 minutes. I had talked to some other friends of mine, they'd never encountered this type of problem. I was lucky enough to eventually get it to work, but it's still unfair that apps like this leave students like me in the dark. [VIDEO ENDS]

Thank you for watching these two videos. I've watched them so many times and shared them so many times, and they're always so horrifying to me. I think it's just like it's completely unethical that these tools are being used. And unfortunately, these tools are used on millions of students per week. Both of these videos relate specifically to the use of Proctorio. Proctorio is the technology that both of them talk about. Proctorio is the only technology I have ever heard of that isn't usable by people with dark skin. And we'll see just how often people with dark skin have those issues.

This is a screenshot from Proctorio that Amaya Ross took showing the webcam test. There are seven images or sorry, nine images on this screen, and out of them, you can see that seven are outlined in red. That means that Proctorio was not able to detect a face in these images. And for those of you that are sighted, you can see clearly faces in all of these. There's just no question about it. So this is why we can't be outsourcing decision-making to AI tools because it can lead to harm like this. And with no human in the loop, students don't have recourse. They don't have someone that they can turn to help.

The final voice that I'd like to centre today is Lucy Satheesan. Lucy Satheesan is a Miami University student and she had an interesting experience with Proctorio too. She analyzed the public source code in the Google Chrome extension and found that Proctorio was using open source facial recognition software called OpenCV. She tested OpenCV against an open source image database of faces called FairFace and found that it could detect black faces less than half of the time. It was actually quite terrible at detecting faces at all, but you can see from this chart that under half of the time it could detect a black face. Proctorio claims without evidence that this finding has been debunked. Actually, it hasn't been debunked.

There is brand new research specifically into OpenCV, the system that Proctorio used or uses, I'm not sure, that shows that this is from the abstract, failure rates. The failure to detect rate increased from just 0.28% for subjects with the lightest skin in our sample to 24.34% for subjects with the darkest, controlling for other factors. And when you include head coverings and glasses, people with dark skin who have head coverings and glasses, the failure to detect

orate skyrockets to over 75%. On the left hand side, there are three gentlemen with head coverings, glasses, and dark skin, and the detector rate is listed as over 75%. On the right are participants with a higher skin lightness score who are seen, whose failure to detect rate is less than 0.5%. So it's like a 150-time difference. It's utterly ridiculous. And Robin wears glasses. So one thing that was so frustrating with the human rights decision was that they couldn't demonstrate that it was racially biased as she complained. There was evidence that showed that maybe it had to do with her wearing glasses, but it actually looks like, according to this new research, it was the combination of her skin colour and glasses that made it so impossible to be seen without shining a flashlight in her face.

This problem is well known within the industry. Respondus, which holds a patent for online proctoring, actually, the patent is for systems and methods for assessing data collected by automated proctoring. The patent shows that they have actually added an adjustment to final tally variable, which when it detects dark skin, applies it, uses a racial detection feature so that a downward adjustment can be made to the final risk tally and on the right is an image of some webcam surveillance from the patent application. What this actually means is that not only is the failure to detect rate very high and you can get kicked out or not have access to your exam, also it affects the flagging that takes place during the exam. Things like eye movement, things like head movement can also be more inaccurate by the failure of these systems to accurately detect people with dark skin. So it's outrageous. We should all be marching in the streets, honestly. But instead, we can focus our advocacy within our institutions and online and publicly and with our colleagues.

So enough was enough for UBC. As I mentioned in March 2021, they banned the software. This was actually a Senate vote in Okanagan and Vancouver that took place on separate days. So citing the risk of discrimination, it was banned effective immediately right before midterms. And that was just, I listened to the discussion live as the senate was talking about this. There was some interesting discussion about, well, shouldn't we just finish using it for midterms and then we can figure it out. But this was shut down by the various participants in the senate because if it's a little bit racist, if it's racist sometimes, how can we possibly justify using it at all? So it was banned immediately.

And so the question as we consider the bias inherent in these technologies is what could we be spending this money on instead? And it's a lot of money.

I did some freedom of information requests to a couple of schools in the United States last year and found that Ohio State University was spending about $200,000 a year, the overall spend. Oh, sorry. I should clarify. So we have purchase orders central to this slide. The purchase order in 2018 was $229,000 in 28. Uh, sorry, 2018: $229,000, 2019: $220,000, 2020: $170,000, purchase orders are what the school is authorized to spend. The overall spend ended up being about $465,531 over the course of several years.

University of Colorado Boulder, has purchase orders totaling $722,000 since 2015. It's unclear to me how much of that was actually spent. But when they reviewed their contract, they found that based on the full-time equivalent enrollment number, $3.68 was being spent per student, whether it was being used or not, and only 5% of instructors were actually using it when the contract was discontinued. So you can multiply that 3.68 by approximately 20 to see what the actual cost was. It's just unbelievable.

Another question that I want to pose to you is does this million dollar software actually stop academic dishonesty? I am very attuned to what students are saying online and discussing online. It's a central focus of my research into this tool, what students are saying. Listening to students is an important part of my practice. There was an article in VICE in 2021 called "Students Are Easily Cheating State-of-the-Art Test Proctoring Tech," which went into many different ways that Proctorio specifically could be circumvented, including the use of a virtual machine, a long HDMI cable, things like a smart watch, smart glasses, the sky's the limit. Students are creative. Even a $0.02 sticky note on your screen can defeat that million dollar software.

Research was done specifically into Proctorio, an article called “On the Efficacy of Online Proctoring Using Proctorio," which came out of the University of Twente in the Netherlands. They had 30 students in their experiment, six of which were asked to cheat in various ways, while five were asked to behave nervously but take the test honestly. And the most important findings were that none of the cheating students were flagged by Proctorio, whereas only one out of six were caught by an independent check by a human agent. So the sensitivity of Proctorio based on this experience should therefore be put at very close to zero. This is all quoted from the paper. "The use of online proctoring is therefore best compared to taking a placebo. It has some positive influence, not because it works, but because people believe that it works or that it might work, work." But of course, students are talking to each other, and they are talking to each other about how it doesn't work, making it worse than a placebo. It's just unwarranted surveillance for no actual reason.

One question that I get a lot and I mentioned it earlier is, what about lockdown browsers? So maybe you've watched this whole presentation and you're horrified by the racism inherent in these tools. But, lockdown browsers don't use your webcam, so are they immune to this sort of criticism? And I can speak to that because when I was an educational technologist, I supported lockdown browsers and I supported students using them directly. My job was to answer the phone when students had an issue with their EdTech, and technical issues abounded with lockdown browsers. Compatibility issues with accessibility software, other browser extensions were common, and they don't actually prevent the use of second devices, so you can just have a phone or a second computer next to your main computer. It's no problem at all to do that, although only students with the resources to do that can. There's the potential for data breaches anytime you use a proprietary tool. But I will say that I think there is an opportunity for a transparent open source tool that is very clear about what it does, does not do and

designed with ethics at its core. A transparent open source tool would actually cost these vendors hundreds of thousands, maybe millions of dollars in business. So that's potentially another motivator for an ethical EdTech developer to consider doing this.

As I mentioned, listening to students is a key part of my practice and something that I encourage everyone to do. There's two Twitter accounts that I created back in 2020. One is twitter.com/Procteario one is twitter.com/ProcterrorU. These are parodies of Proctorio and Proctor U respectively. What I did with these accounts is I simply checked every several days for mentions of the word Proctorio or Proctor U and retweeted examples of students reporting harm. So there are hundreds of tweets that I've retweeted, and each one of them is an authentic story from a student experiencing something awful. So reading those, sharing those stories, I think is really critical, as well as reading the student reviews of these tools, which I've compiled at Googlereviews.linkletter.org.

Centring the student voices that are in these reviews, I'll point out that Proctorio and other remote proctoring extensions have the very worst ratings in the Google Chrome web store. I have not been able to find and I have looked a lot any extensions that have a worse rating than these ones. For example, Proctorio Honorlock, Proctor U. Thousands of students have reviewed Proctorio as one star, and in 2021, I flagged over 1,600 instances of students reporting emotional harm, technical faults, and invasion of privacy. I actually sent a letter including all the flagged reviews to US senators that were investigating Proctorio. You can read my letter, which was unfortunately not really followed up on by these senators at dearsenators.linkletter.org

I have some screenshots here, which I'll read from my analysis. So in yellow, I highlighted terms related to emotional harm, like stress, nightmare, anxious, panic attack. On the right hand side, we have some posts that include, now my testing anxiety has jumped from 10 to 11, invasion of privacy, and stresses students out. I am so upset that my professor chose to use this in the first place. It's a gross invasion of privacy and wholly unnecessary, and it doesn't even work a majority of the time.

In orange, I flagged reliability and quality issues like bugs, crashes, glitches. On the right, we see this thing is f-ing terrible, have to use it for university tests. It always crashes, crashed my PC many times.

And in red, finally, I highlighted terms related to human rights like invasion of privacy and violation of privacy. And we see words on the right, like in violation of privacy, invasion of privacy, terrible, intrusive, and the CEO doesn't care about student privacy.

So wrapping up my presentation now, my first presentation now, I just want to urge you to please listen to students. If you're not hearing their voices, ask them what they think. If you're in a room where decisions are being made and there's no students in the room, make a

statement that students should be included. I just urge you please to listen to students and hear what they have to say.

So I thank you for being here. Together, we've considered trust, transparency, equity, and care as lenses through which to evaluate the ethics of remote proctoring. And so I thank you very much for being here. This concludes my first presentation.

All right, so my second presentation is called Protecting Students from AI with Algorithmic Impact Assessments. How BCIT did it?

So Canada has an algorithmic impact assessment tool, which is a questionnaire that determines the impact level of an automated decision system. It's composed of 51 risk and 34 mitigation questions, and assessment scores are based on many factors, including the system's design, algorithm, decision type, impact, and data. The tool helps assess and mitigate risks, ensure transparency, accountability, and fairness in automated decisions. And the government has actually. Oh, thank you. If you're signing off, no problem, the recording will be available. And it's mandatory for federal departments and agencies that use automated decision systems. Similar to a privacy impact assessment, algorithmic impact assessments may be something that can be incorporated into PIAs, but the idea is that they have their own objectives. And my question to you is, and we're going to look at the tool. If this tool exists, what's stopping us from using it? If we can prevent harm, why wouldn't we do it?

And so let's talk about some harm that took place at McMaster University. This is the nightmare scenario that none of us want to deal with where a student makes a complaint to the Privacy Commissioner and we have to defend our use of surveillance software. So McMaster University uses Respondus Lockdown Browser and Monitor. It's Lockdown and AI monitoring. A student complained to the Information and Privacy Commissioner of Ontario and did not want to share their identity with McMaster, so the IPC initiated an investigation. They found that the vendor used video surveillance to improve the services. That was in their privacy policy. But the IPC found that those video recordings are actually personal information because of course they are. Your face is personal information, your voice is personal information. The things in the background of your video can be personal information. So the vendor found that this use of personal information did not fall under the educational purpose that was authorized by the Privacy Act in Ontario. Students never consented to it and they had no opportunity to opt out. So the IPC recommended that McMaster protect its students from the heightened risks of AI-enabled tools by conducting algorithmic impact assessments. McMaster University is now conducting algorithmic impact assessments or AIAs, having adopted the Canadian tool. University of Ottawa scholar Teresa Skaza has an amazing post summarizing this complaint and what it says. It's like 50 pages. But unfortunately, her website is down right now. So in my links, I have an archive.org link that will work.

The Canadian AIA tool states that departments are responsible for releasing the final results of the AIA in an accessible format and in both official languages on the Open Government Portal, which really goes to show that we should be transparent with our use of these technologies and our mitigation strategies for eliminating bias. And there's no better way to do that than to put them online. My experience with the privacy library has been that institutions are very hesitant to share their PIAs for reasons like, Oh, well, somebody could use our PIA to hack the system. With AIAs, that's not an excuse because what are they going to do? Be aware that a system is biased and take mitigation steps. This is an awareness tool. This is a tool that's used to do the right thing to do the ethical and honourable thing and it shouldn't be kept secret.

Right now, there are 29 algorithmic impact assessments publicly available from organizations including Immigration Refugees and Citizenship Canada, Public Health Agency of Canada, and a BCIT librarian. If you go to bit.ly/bcitaia1, I'm going to type this one into the chat. You'll actually see a PDF document, the export file from the AIA that I conducted independently. This is a really important point because this survey tool is designed to take about 35 minutes to do. So there's actually nothing stopping an educational technologist with really good understanding of how these tools work from doing it themselves. There's nothing stopping us. We can do these ourselves for the remote proctoring tools and surveillance tools in place at our school. And perhaps by doing so, we'll have leverage. We'll have a way to advocate within our institution for better mitigation strategies or more awareness of the harms inherent in the tools. So there's no reason to go through a formal process. You can actually do this yourself and start having conversations.

McMaster's approach was something that was influential to us at BCIT. So I'm the vice chair of our Educational Technology and Learning Design Committee and I met with McMaster University, and they shared documents with us, including their privacy risk check for early stage flagging, their privacy risk assessment tool, which combines AIAs with PIAs, their contract language, limiting vendor use of data. They actually will not accept contracts that have that for use, improving the product language, that needs to be removed if you're going to do business with them. It defines PII as including biometric info like your face, your voice, your body, your movements, which I think is a really important step.

They broke it down. What they scrutinize, what they analyze is the system, the algorithm, the decision made by the algorithm, the impact of the decision, the data used to make that decision, and the mitigation to reduce the harm.

And this is what we used at BCIT for our AIA initiative, the race to protect students, I call it.

So our EdTech and Learning Design Committee decided to pilot algorithmic impact assessments, and we chose two automated decision systems that are already in use. One is Integrity Advocate, which is BCIT’s remote proctoring software, and the other was Turnitin. We banned Turnitin's AI detector in 2023, but it does still have a plagiarism detector which arguably

makes automated decisions. And so we formed a subcommittee with representation from the Learning and Teaching Centre and Educational Technology Services. Shout out to Paul Krampitz, Kyle Hunter, and Eric Aram, chair of the committee for all of their participation and leadership. And we completed two AIAs in two meetings with me leading the one on Integrity Advocate.

Ultimately, after the AIAs were shared back to the committee, we decided to oh, sorry, this is a repetitive slide. But we endorsed an AIA requirement for new decisions around EdTech tools. And Education Council, I'm very proud to say, recently endorsed AIAs. So at the institute level, AIAs are now official. No new educational technology that makes automated decisions will be approved or even considered without the completion of an AIA first. And we have a policy, policy 5,900 that gives the ETLDC essentially a veto power, approval power over new EdTech that comes in. So using the combination of AIA requirements and policy 5,900, we're able to stop this stuff before it even gets in the door, and we're prepared for things like the next pandemic, the next terrible decision by a company like Google to add an AI button. That happened recently. We're ready to protect students.

I was going to go hands-on with the tool, but I think at this point, what I'm going to do is conclude my second presentation.

It's really been an honour to be part of the EdTech Sandbox Series. Bye everyone. Thank you for being here.