Online proctoring tools are a violation of privacy and a great risk to students, leaving them forced to choose between academic progress or a high risk of exposure to malware and other unwanted programs that will have access to files on their computers. It leaves your computer and all your info extremely vulnerable to theft and viruses. When the proctoring tool fails to work properly, students have been prevented from completing their exams. Furthermore, the software that many post-secondary institutions are using places the responsibility for any damages on the student in their terms and conditions, and they reserve the right to sell the information they collect from your computer. See below for excerpts from the terms of service for the largest proctoring software used by universities, ProctorU.

(source: https://www.proctoru.com/terms-of-service)

- Neither ProctorU nor its vendors, affiliates, or any person associated with ProctorU makes any warranty or representation with respect to the [...] security, or reliability of the Services...
- Neither ProctorU nor anyone associated with ProctorU represents or warrants [...] that the Services are free of viruses or other harmful components...
- ProctorU does not assume any liability for loss or damage to your computer systems, devices, or networks as a result of your use of the services.
- ProctorU will not be liable for any loss or damage caused by a distributed denial-of-service attack, viruses, or other technologically harmful material that may infect your computer equipment, computer programs, devices, or data due to your use of the Services.
- YOUR SOLE REMEDY AGAINST PROCTORU FOR DISSATISFACTION WITH THE SERVICES IS TO STOP USING THE SERVICES.

Another popular service, ‘Examity’, has the following in their terms of service:

(source: https://examity.com/website-privacy-policy/)

- Information We Collect: [...] Information that you provide directly to us by filling in forms on our Website, including your name, email address, street address, telephone number, or other information.
- We cannot guarantee that it will be 100% secure. Your transmission of your data to our Website thus is done entirely at your own risk.
- We may disclose your personal information to third parties if we are involved in a merger, acquisition, or sale of any or all of our business and/or our assets to a third party...

Other available platforms generally have similar policies that can be summarized as:

1.) We will collect all personal information gleaned from both registration and use of our software
2.) We will not guarantee that our service or our stored data of your personal information is secure or safe
3.) We reserve the right to transfer all collected personal information to additional unknown parties under acquisition, merger, or bankruptcy.

4.) Your only recourse against any of these conditions is to refuse our service.

Regardless of whether you have sensitive work or financial data, we as students should not be forced to potentially compromise our privacy or security with virtually no guarantee of even basic vetting from these third-party companies. Agreeing to these terms allows companies to sell your data and have no liability for any damages caused by the sale.

See below for an article from The Verge, on the privacy violations and environment created by the proctors during an exam written with Examity

(Sourced from: https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education)

Below is a summary of some key points from this article:

- Examity would store a biometric template of student's keystrokes.

- Students were forced to display both sides of their driver's license in the webcam's view.

- A proctor has admitted to viewing personal information and messages on students' screens before.

Note that this list is not exhaustive.

But the company's attitude toward personal data is concerning; its privacy policy states that Examity may collect a number of personal details from students who test with it, including student names, addresses, biometric records, driver's license numbers, and passwords. The company can use such details to analyze usage patterns and share them with third parties.

Examity's privacy policy is clear that the company can't guarantee the security of personal data. "Your transmission of your data to our site is thus done entirely at your own risk,". That is, Examity takes no responsibility for protecting students' personal data, which they are required to provide in order to write midterms and exams.

While McMaster has not confirmed which software they will be using, proactive measures should be taken to ensure that best practices are followed. I would like to motion for the MSU to make an official statement demanding that any online proctoring tool used by the university comply with the following requirements, and possibly condemning the use of tools which do not satisfy all of these requirements:

1. Compliance with the law. The supplier must explicitly agree to comply with applicable privacy laws regarding the collection, use, processing, storage, disclosure and retention of personal information.

2. Robust administrative, physical and technical safeguards. The terms of use should explicitly describe the ways in which personal information is secured against unauthorized access, use and

disclosure. Robust safeguards include but are not limited to: data security policies, firewalls, industry standard SSL or TLS encryption, virus and intrusion detection, authentication protocols, third-party penetration testing, security audits and training.

3. Retention and destruction of data. The retention of personal information should be limited to the shortest duration possible so as to comply with statutory requirements and/or to satisfy clients' needs.

4. Permissible uses of the data. Personal information that is collected by the supplier should be used for the limited purposes of:

   (i) that for which the end user has granted permission;

   (ii) that which is necessary to deliver, update and improve the services; and

   (iii) that which is required by applicable law.

   Wherever possible, statistical or aggregate information collected about the use of the services should not be linked to identifiable personal information.

5. Disclosure to third-party companies. Third parties should be prohibited from accessing or using personal information with limited exceptions. Exceptions should only be made for third parties who are explicitly identified and authorized by the end user (students). These parties should agree in a contract to maintain the recordings in confidence and under terms at least as strict as the terms of the supplier's policies and agreements. Recordings should be stripped of, and not contain, any personally identifiable information, and should only be used for the sole purpose of delivery or enhancing the services.

6. Security breach reporting. The privacy policy should outline the supplier's incident response management plan for reporting, responding to and containing breaches or suspected breaches where personally identifiable information may have been compromised.

7. Indemnity for security breaches. Although infrequent, a supplier will provide a full indemnity to McMaster and/or the end user for all security breaches resulting in a breach of personal information. Typically, liability for security breaches is fixed at a nominal amount of damages and is predicated on a finding of negligence or willful misconduct on the part of the software company. McMaster should seek to enshrine the supplier's commitment to cooperate with McMaster in the event of a security breach.

8. Residency of the data. A reasonable attempt must be made to ensure that data will remain in Canada, and software which does not retain information domestically must take liability and responsibility for data storage and transfer to locations outside of Canada. Otherwise, selecting a

supplier who operates in Canada, processes data in Canada and stores data on servers located in Canada is a “good to have” feature as it reduces exposure in the event of a security breach.

In order to follow best practices and ensure the best experience for students, I also request that the following are implemented internally alongside any proctoring software used by McMaster:

1. Transparency. McMaster must implement a FAQ which will provide the legal terms in plain language and without bias, while also preemptively responding to student queries.

2. Guidelines. That restrict the internal use of this data by individuals within the McMaster community to a reasonable extent.

3. Accessibility. Faculties which choose to use online proctoring software should designate a staff member who will be responsible for the resolution of student-related concerns, and

4. Consideration. Students should not have to be forced to risk their privacy. Reasonable consideration must be made for students who refuse to use the software or whose device is not equipped with a functioning camera and microphone.

There is no perfect, impenetrable technology that dispenses with all risk. McMaster must take responsibility in determining whether the privacy risk is reasonably mitigated by contractual, administrative, physical and technical safeguards employed by the supplier and the university.