Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PI21-00001

McMaster University

February 28, 2024

Summary: The Office of the Information and Privacy Commissioner of Ontario (the IPC) received a complaint about McMaster University's (McMaster or the university) use of Respondus exam proctoring software under the *Freedom of Information and Protection of Privacy Act* (*FIPPA* or the *Act*). The software comprises two programs. Respondus LockDown Browser limits what users can access on their computers and Respondus Monitor analyzes audio and video of students during the exam to scan for possible cheating. The complainant did not want the IPC to provide their name and complaint to the university, so the IPC opened this Commissioner-initiated complaint to address the university's use of this exam proctoring software.

This report concludes that conducting exams and appointing examiners is a lawfully authorized activity of the university. Proctoring exams online to ensure their integrity is an appropriate component of conducting certain types of exams and is therefore also a lawfully authorized activity. On the question of whether the collection of personal information through the use of Respondus exam proctoring software is necessary to proctor exams, I find that Respondus LockDown Browser collects little personal information, and only collects and uses what it needs to function. Respondus Monitor collects more sensitive personal information, including biometric information, and uses artificial intelligence (AI) technology, which carries heightened concerns. Because the personal information collected by Respondus Monitor on behalf of the university is necessary for that tool to fulfill its function of exam proctoring, it is authorized under section 38(2) of the *Act*. However, the university has not provided adequate notice for its collection of personal information as required by section 39(2) of the *Act* and the use of students' personal information through Respondus Monitor is not in compliance with section 41(1). Moreover, the current contractual arrangement between the university and Respondus is contrary to section 41(1) of the *Act* in so far as it does not adequately protect all of the personal information collected

and allows Respondus to use personal information for system improvement purposes without the consent of students.

In this report, I make a number of recommendations for the university to bring itself into compliance with the *Act*. Given the heightened risks associated with AI technologies, I also recommend that the university adopt additional guardrails around its use of Respondus Monitor and incorporate these stronger protections into its ongoing use of the software and any future agreement with Respondus.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990; R.R.O. 1990, Regulation 460; *McMaster University Act*, 1976

Orders and Investigation Reports Considered: Investigation Report 196-057M and Privacy Complaint report PR16-40.

Cases Considered: *Cash Converters Canada Inc. v. Oshawa*, 2007 ONCA 502.

BACKGROUND:

[1] In January 2021, the Office of the Information and Privacy Commissioner of Ontario (the IPC or this office) received a complaint from a student at McMaster University (McMaster or the university) regarding its use of proctoring software for exams conducted remotely and online. The software being used was Respondus LockDown Browser and Respondus Monitor, both from the vendor, Respondus.

[2] The student raised concerns that McMaster was inappropriately collecting student data via this software and was unsure how the university was using, disclosing and disposing of student personal information gathered via this software.

[3] The student did not consent to the IPC sharing their name and a copy of their complaint with the university. As such, the student's complaint file was closed and this Commissioner-initiated file was opened to address the university's use of proctoring software.

[4] The complaint was brought in January 2021 during the height of COVID-19 related restrictions.[1] The university stated that it began using Respondus Monitor and Respondus Lockdown Browser to administer remote assessments in 2020, the first year of the COVID-19 pandemic. McMaster continued to hold classes virtually through the bulk of 2021[2], with 50% of course components returning to on-campus attendance as of September 2021.[3] The Omicron wave caused a temporary reversion to remote learning

[1] See, for example, the additional emergency measures put in place on January 13, 2021: https://news.ontario.ca/en/release/59922/ontario-declares-second-provincial-emergency-to-address-covid-19-crisis-and-save-lives

[2] https://covid19.mcmaster.ca/spring-summer-and-intersession-2021-terms-to-be-held-virtually/

[3] https://provost.mcmaster.ca/app/uploads/2021/09/McMasterU-Continuity-of-Education-Plan-2021.pdf

for a brief time between December 2021 and January 2022.[4] However, as of January 31, 2022, Ontario's phased re-opening plan saw restrictions begin to ease.

[5] Respondus Lockdown Browser and Respondus Monitor programs are often used together, though Respondus LockDown Browser can be used on its own.

[6] Respondus describes Lockdown Browser as a custom browser that locks down the testing environment within a learning management system.[5] The user must install this software, and when in active use it displays the assessment full screen and locks some functions of a student's computer to discourage cheating. During assessments, students are unable to conduct an internet search, access files on their computer, navigate away from the assessment screen, or use the copy-paste, messaging, screen sharing, or print screen functions. Lockdown Browser does so by making changes to local settings on students' computers to temporarily control or restrict access to computing resources.

[7] Respondus Monitor accesses a student's webcam and records them during assessments, acting as a form of virtual invigilation. The recordings, including biometric information, are analysed using artificial intelligence (AI) to flag activities it deems suspicious or consistent with cheating. Instructors are provided with a report of flagged events for their review. The inclusion of a suspicious activity flag does not necessarily mean that the student was cheating. Instructors may request to review the exam recording via McMaster's Academic Integrity Office and speak to the student to assess whether there was potential academic dishonesty that should be referred as a possible breach of McMaster's Academic Integrity Policy.

[8] On July 17, 2020, McMaster publicly released "Privacy & Information Security Impact Assessment Report – Online Proctoring: Respondus"[6] (PIA Summary) which provided background, analysis, and key findings and recommendations from this assessment report.

[9] In that PIA Summary, McMaster outlined the challenges of the COVID-19 public health emergency, including its resulting inability to deliver in-person examinations with proctors or invigilators. While some instructors were able to use existing tools to conduct exams or other evaluations, the university noted that these solutions were unlikely to fill the needs for all courses, including accredited courses. To address this gap, the university launched a pilot project and evaluation of online proctoring options to find a preferred approach for fall 2020. The PIA Summary notes that the university conducted a preliminary risk assessment of Respondus in June 2020, followed by an In-depth Risk Analysis later that same month. Based on the key findings and recommendations in that PIA Summary, McMaster contracted with Respondus to provide online proctoring for exams.

---

[4] https://president.mcmaster.ca/mcmaster-community-december-2021/
[5] https://web.respondus.com/he/lockdownbrowser/
[6] https://secretariat.mcmaster.ca/app/uploads/PIA-Report-Online-Proctoring-Respondus.pdf

[10] Among the key findings of the PIA Summary were that individual students should be able to make arrangements if they require an accommodation, and that Student Accessibility Services should have an opportunity to identify those accommodation requirements to the service provider. The PIA also indicated that the application must only be installed for the duration of the exam and may be removed afterwards, and that for courses using Respondus, the course outline should clearly communicate its use to students.

[11] Also pursuant to the PIA Summary, McMaster made arrangements for students to access Respondus through the University's Avenue to Learn portal, rather than requiring students to create individual accounts to access the software. This dispensed with the collection of students' individual contact information by Respondus.

[12] McMaster set out three separate criteria for the use of Respondus software, which apply to both Respondus LockDown Browser and Respondus Monitor:

- The course is accredited;
- The course is mandatory; or
- The class size and/or assessment method dictates its use.

[13] I note that the criteria above do not include the presence of COVID-related restrictions. Under these parameters, McMaster allows the continued use of Respondus LockDown Browser and Respondus Monitor post-pandemic as long as one of the three conditions is met.

[14] Regarding the first condition, McMaster notes that accreditation is determined by a third party where a course or program must meet certain standards to satisfy professional and regulatory requirements. Proctored invigilation may be one of the conditions set out for such a course. McMaster offers a range of accredited programs, including nursing, psychology, rehabilitation, social work and engineering. McMaster states proctored exams may be a requirement for professional certification in these fields.

[15] Regarding the second condition, McMaster notes that only some courses are mandatory to obtain a degree; others are elective. Assessments for mandatory courses are identified as essential assessments and are eligible for Respondus use.

[16] Finally, regarding the third condition, McMaster has determined that Respondus may be used based on the nature of the assessment required, or the size of the course itself. Courses that have a large class size are eligible for online proctoring, as are those that require person-to-person assessment, such as languages.

[17] McMaster, on its own behalf and through its associated MacPherson Institute, has provided guidance to instructors who are considering using Respondus software. The guidance provides in part as follows:

> Respondus monitors students while they are completing online assessments with an aim to ensure academic integrity. However, the decision to use Respondus should not be taken lightly. Please ensure you have considered the following:
>
> - Rationale: do you really need to use online proctoring? Unless a proctored assessment is a requirement for a professional certification, you should consider alternate assessments or, if you rely on quizzes and tests, refer to our Guide to Tests and Exams Using Avenue to Learn on how you can configure tests and quizzes to increase fidelity without having to use a proctoring technology.
>
> - Communication: have you included a statement as to your rationale and use of online proctoring in your course syllabus? Will you ensure instructions on how to use are provided to students along with a practice quiz?
>
> - Accommodation: Quizzes that use Respondus can be configured on Avenue to Learn for accommodation purposes, but you will also need to develop a Plan B for certain accommodations or if technical/connection issues arise.
>
> - Mental health and well-being of your students: consider the added layer of anxiety online proctoring can promote and how to support students through this.[7]

[18] The university also recommends that instructors explore other alternatives to proctored exams, including take home exams, projects, reflections, group work, guided online discussions, and peer-reviewed activities.

[19] If an instructor wishes to use Respondus software, they must apply in advance to use these tools in their course. The application must identify which service they wish to use and provide a rationale for this use. The instructor must also confirm that they have notified their students of their intention to use Respondus as an online monitoring tool.

[20] The responsible IT manager reviews this application. If they identify any concerns that the request falls outside the university's criteria for the use of Respondus, they are to consult with the privacy office and provost's office on the matter.

[21] In its online FAQ[8] directed to instructors, McMaster addressed how Respondus software works, information about the flags in the post-exam reports provided to instructors, and what instructors should do in such instances. In addition to the

---

[7] https://mi.mcmaster.ca/respondus/

[8] https://avenuehelp.mcmaster.ca/exec/respondus-lockdown-browser-and-respondus-monitor-instructor-faq/

information provided on its website, McMaster states that it informed instructors of the availability and limitations of the use of Respondus software via faculty channels.

[22] McMaster also provided information to students by publishing resources online, including "An Introduction to Respondus."[9] This includes sections on why Respondus is being used, the data that is being collected, and the relevant privacy and data retention practices. It also directs students to additional resources if they have any concerns.

[23] "Writing a Test Using Respondus"[10] is another online resource provided by McMaster. It provides information on the steps to take before, during, and after a proctored exam. It also provides information regarding how the information gathered from the recordings is used by the university after the test is complete. It notes that the instructor receives a spreadsheet that summarizes any flags during the test. The instructor is to review the flags and begin a conversation with the student if there is a concern. It notes that the student's video is only reviewed by the instructor upon the instructor's request and if appropriate.

[24] This is consistent with the information that McMaster provided to the IPC. McMaster stated that instructors cannot access recordings from the exam sessions without authorization from the Academic Integrity Office pursuant to an academic integrity investigation. Otherwise, instructors do not receive copies of the recordings, and have no ability to access them.

[25] McMaster noted that since it began using Respondus Monitor in 2020, there have been two cases where recordings were reviewed as part of an investigation. The university stated that in both cases, the students were charged with academic integrity misconduct, and the recordings were integral in providing evidence documenting the misconduct. McMaster also takes the view that the use of the software generally deters students from engaging in inappropriate activity as they know their actions can be viewed.

[26] McMaster has provided alternative assessments for students who have registered for academic accommodation with Student Accessibility Services. The accommodation was for assessment without artificial intelligence monitoring, in which the university provided human proctoring via Zoom for 34 students in the 2020/21 academic year, and 32 students in the 2021/22 academic year. According to McMaster, there were no accommodation requests for in-person proctoring in 2022-23.

ISSUES:

[27] The following issues have been identified as arising from this investigation:

---

[9] https://mi.mcmaster.ca/app/uploads/2021/03/An-Introduction-to-Respondus-_updated.pdf

[10] https://mi.mcmaster.ca/app/uploads/2021/03/RESPONDUS-Writing-a-Test-Using-Respondus-Updated.pdf

1. Is the information at issue "personal information" as defined by section 2(1) of the *Act*?

2. Was the collection of the personal information in accordance with section 38(2) of the *Act*?

3. Is the notice of collection in accordance with section 39(2) of the *Act*?

4. Was the use of personal information in accordance with section 41(1) of the *Act*?

5. Does the university have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students, in accordance with the requirements set out in section 4(1) of Ontario Regulation 460 and sections 4(1) and 5 of Ontario Regulation 459, made pursuant to the *Act*?

DISCUSSION:

Issue 1: Is the information at issue "personal information" as defined by section 2(1) of the *Act*?

[28] McMaster was asked to describe the information Respondus collects via the students' use of Respondus Monitor and Respondus LockDown Browser. McMaster stated that as of fall 2020, students could access both Respondus programs by logging into the McMaster "Avenue to Learn" portal, eliminating the need for students to provide individual contact information. The university separately provides the vendor with the student's name and the course codes.

[29] During the assessment process, Respondus LockDown Browser does not routinely collect information. The exceptions are 1) when a student ends an exam session early, in which case they must provide a reason for doing so; and 2) if a student requires technical support and accesses the Respondus Help Center.

[30] At the start of each assessment session, students are required to provide photo identification, and Respondus Monitor captures this image. This software records audio and video of students throughout the exam session, which includes collection of students' biometric data.

[31] The university provided the following description of the biometric data collected:

> The biometric data collected by Respondus Monitor include facial expression, body posture and positioning, direction of the test takers (sic) eye-gaze, and verbal elements. These elements are tracked and recorded to document when a student may have an unauthorized text or tool (e.g. cell phone), or unauthorized conversation regarding the answers in an assessment event.

[32] Under section 2(1) of the *Act*, "personal information" means recorded information about an identifiable individual, including,

> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
>
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> (c) any identifying number, symbol or other particular assigned to the individual,
>
> […]
>
> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

[33] McMaster has agreed that the video recordings, course information, and biometric elements are students' personal information. I agree and find that the accompanying audio recordings should also be considered personal information.

[34] McMaster did not take a position on whether students' names, provided as part of the use of Respondus Lockdown Browser, were also personal information. I find that names, taken together with course information, are personal information pursuant to section 2(1)(h) of the *Act*. I also find that the photo identification captured by the video recording is personal information pursuant to sections 2(1)(a) and 2(1)(c) of the *Act*.

[35] In summary, I find that the students' names, course information, biometric data, photo identification, and audio and video recordings are "personal information" as defined in section 2(1) of the *Act*.

Issue 2: Was the collection of the personal information in accordance with section 38(2) of the *Act*?

[36] Section 38(2) of the *Act* prohibits the collection of personal information other than in the following circumstances:

> No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

[37] McMaster has agreed that Respondus was acting on behalf of McMaster when it collected the students' personal information via the use of Respondus LockDown Browser and Respondus Monitor.

[38] When asked for the university's authority for the collection of this personal information, McMaster referred to section 13(h) of the *McMaster University Act*[11], which states that "[the] Senate has power to… conduct examinations and appoint examiners." McMaster also provided guidance documents addressing undergraduate and graduate exam policies.

[39] From this response, McMaster appears to be taking the position that the collection of personal information is either expressly authorized by statute under the second branch of section 38(2) or necessary to the proper administration of a lawfully authorized activity under the third branch of the same section. I address both these grounds.

Expressly authorized by statute

[40] Previous IPC reports have addressed what constitutes collection that is "expressly authorized by statute". In Investigation Report 196-057M, the identically worded provision of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) was interpreted as follows:

> [In] our view, the phrase "expressly authorized by statute" in section 28(2) of the Act requires either that specific types of personal information collected be expressly described in the statute, or a general reference to the activity be set out in the statute, together with a specific reference to the personal information to be collected in a regulation under the statute; i.e., in a form or in the text of the regulation.

[41] This interpretation has been upheld and applied by the Ontario Court of Appeal in *Cash Converters Canada Inc. v. Oshawa (City)* ("*Cash Converters*").[12]

[42] The provision of the *McMaster University Act* setting out its power to conduct examinations and appoint examiners does not address the university's power to collect specific personal information for this purpose, and the university did not identify any regulation to this effect. Based on the information before me, I find that the collection of student personal information by Respondus software on behalf of the university was not expressly authorized by statute.

Necessary to the proper administration of a lawfully authorized activity

[43] *Cash Converters* is also the leading authority on the interpretation of the third branch of section 38(2) which I refer to as the "necessity test". The Court's reasons in

---

[11] *McMaster University Act, 1976*, as amended by Bill 173, Chapter 5, S.O. 2016

[12] 2007 ONCA 502, at paras. 36-37.

that case make it clear that the necessity test has two requirements to be addressed separately and in the following order:

1. Is the activity engaged in by the institution a lawfully authorized activity? If the answer is "No", the collection does not comply with the statute.

2. If the answer to question 1 is "Yes", is the collection of the personal information necessary to the proper administration of that activity?

[44] To satisfy these two requirements, an institution must identify the lawfully authorized activity in question, and then explain how the collection of personal information is necessary to its administration.

Lawfully authorized activity

[45] As mentioned above, section 13(h) of the *McMaster University Act* sets out the university's power to conduct examinations and appoint examiners. While this provision is the source of the university's power, it does not represent the full scope of its lawful authority flowing from the power to conduct exams. Sections 78 and 79 of the *Legislation Act* expand beyond this explicit authority as follows:[13]

> Incidental powers
>
> 78 If power to do or to enforce the doing of a thing is conferred on a person, all necessary incidental powers are included.
>
> Performance when occasion requires
>
> 79 Powers that are conferred on a person may be exercised, and duties that are imposed on a person shall be performed, whenever the occasion requires.

[46] As explained in *Cash Converters*, a general power given to a public body by statute should be given "a broad and generous interpretation" that allows it to achieve its legitimate interests.[14]

[47] There can be no doubt that the university's lawful authority to conduct examinations includes the incidental power of proctoring these exams to ensure their integrity. The question then arises whether *online* proctoring is itself a lawfully authorized activity.

[48] I am not aware of any principle of statute or common law that would confine the method by which the proctoring of examinations may be conducted by McMaster to an in-person setting, or that would be lead me to conclude that online proctoring is not a

---

[13] 2006, SO 2006, c 21, Sch F, ss. 78, 70.
[14] *Cash Converters*, at para. 24.

lawfully authorized activity. I find that online proctoring was a lawfully authorized activity when in-person learning was not possible during the COVID-19 pandemic. Although it is now possible to resume in-person invigilation post-COVID, I accept that there may be other legitimate reasons why the university would continue to use online exam proctoring as a means of fulfilling its statutory authority to conduct examinations in circumstances that have significantly changed since the pandemic.

[49] The university has a legitimate interest in trying to ensure academic integrity by identifying and deterring cheating in exams. McMaster provided statistics showing an upward trend in academic integrity cases, with a spike in the 2020-21 academic year. The university provided an explanation for why it believed this increase had occurred:

> As you can see, the Office of Academic Integrity has seen an increase in student academic integrity issues during the pandemic. This is not surprising, as other institutions are reporting the same, but it is a challenge that the university needs to address. There are a number of contributing factors including: increasing ease of online collaboration (Reddit, SnapChat, WeChat, Discord, texting), companies that facilitate contract cheating and collaboration during tests (Chegg, Course Hero); attitudinal changes in students; more online testing tools; and an increasing pressure and anxiety experienced by students. These factors have been amplified during the pandemic due to remote course delivery and increased community stressors.

[50] While the academic integrity concerns noted above may have been amplified during the COVID-19 pandemic, they are not all specific to pandemic-related conditions. I accept that by incorporating online proctoring into its evaluation methods, McMaster was also attempting to address other new challenges that arise in an increasingly digital and remote learning context.

[51] Consequently, while I accept that the inability to conduct in-person examinations during the COVID-19 pandemic was the initial impetus for McMaster adopting the Respondus software to proctor online exams, the removal of that public health limitation does not render collection unlawful at the first step of the analysis under section 38(2).

Necessary to the proper administration of the activity

[52] The next question is whether it was necessary for McMaster to collect the personal information that it did, via the use of Respondus software, for the purposes of conducting and proctoring exams.

[53] The test for determining whether this second requirement is satisfied was articulated by the Court of Appeal in *Cash Converters* as follows:

> … [T]he institution must show that each item or class of personal information that is to be collected is necessary to properly administer the

> lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not "necessary" within the meaning of the *Act*. Similarly, where the purpose can be accomplished another way, the institution is obliged to choose the other route.[15]

[54] I now turn to examine the functionality of Respondus Lockdown Browser and Respondus Monitor separately to determine whether the collection of each item or class of personal information was necessary for the purpose of conducting and proctoring online exams. I note that the findings below are specific to the Respondus software at issue in this case, and may not apply to other online proctoring software, which would be subject to their own analyses.

Respondus LockDown Browser

[55] In-person proctoring generally involves a controlled environment combined with invigilators who observe the test-takers. Similar to the controls present in an examination room, Respondus LockDown Browser works by providing a controlled environment, placing the student in a setting where they cannot easily access outside resources. Once in place, Lockdown Browser holds the computer environment secure but does not collect more than a minimal amount of the student's information, namely the student's name and course number, and certain additional information if a student ends the exam early or accesses the Respondus Help Center.

[56] I accept that the university is obliged to put such limits in place during online examinations, just as it does during in-person exams. I find that the limited personal information that the Respondus LockDown Browser collects is necessary and proportional for that purpose. Given how closely the information collected by LockDown Browser corresponds to the information provided by students during in-person exams, the University has demonstrated that LockDown Browser meets the necessity test whether exams are administered in person or online.

[57] I am therefore satisfied that the limited personal information collected on behalf of the university via the use of Respondus LockDown Browser is authorized as being necessary under section 38(2) of the *Act*.

Respondus Monitor

[58] Respondus Monitor collects a student's name and identification, as well as audio and video recordings of the student. In addition, during the examination, Respondus Monitor captures a student's biometric information in real time, including students' movements and behaviour, and analyzes this information via an AI-enabled algorithm. It then produces a report to the university which flags certain events that may indicate instances of academic dishonesty.

---

[15] *Cash Converters*, at para. 40.

[59] To provide this service, Respondus Monitor has to be able to ascertain who is taking the test and collects student identification information for that purpose. Moreover, Respondus Monitor has to collect the required biometrics (which include facial expression, body posture and positioning, direction of gaze, and verbal elements) for its algorithm to assess and flag suspect behavior. Respondus also has to capture audio and video recordings of students while taking their exams to give instructors the ability to review first-hand any exam sessions which have been flagged. Otherwise, the university would not be able to provide human oversight of the algorithmic assessment, which is key to ensuring McMaster remains accountable for the use of this software.

[60] I accept that for McMaster to use this exam proctoring service, the individual items and classes of personal information collected by Respondus Monitor on behalf of the university were technically necessary for the purpose of conducting and proctoring the exams. I am satisfied that under current law, the collection of personal information by Respondus Monitor was necessary for the proper administration of the university's lawfully authorized activity of conducting and proctoring online exams both during and post pandemic.

[61] The resumption of in person learning does not change the facts that the items or classes of personal information that Respondus Monitor collects are required for this proctoring tool to function and that Respondus Monitor collects only the information necessary for it to function. Accordingly, I find that the University's collection of personal information through Respondus Monitor is in compliance with section 38(2) of the *Act*.

Residual Concerns about the use of Respondus Monitor software

[62] To be clear, this does not mean I am unconcerned with the University's continued use of Respondus Monitor. I am keenly aware of the heightened privacy risks associated with automated online exam proctoring, as compared to in-person tests. A human proctor in an exam room observes many students in a neutral setting and does not generally record information regarding the individual students. Respondus Monitor, in contrast, is focussed on each individual student at all times, often in their home settings, potentially capturing extraneous personal information about their living environment and conditions. Through the use of its AI-enabled algorithm, it assesses whether the student may have demonstrated behaviour consistent with cheating. Respondus Monitor may "see" signs of cheating even when there is nothing there, due to the constant input of the student's movements, potential bias in the data sources used to train its algorithms, and potentially inaccurate inferences drawn from such data. This is why instructors are made aware that the report they receive may include false positives.

[63] In response to an earlier draft of this report, McMaster stated that it "retains complete autonomy, authority, and discretion to employ proctored online exams, prioritizing administrative efficiency and commercial viability, irrespective of necessity."

[64] I am troubled by the University's focus on administrative efficiency and commercial

viability "irrespective of necessity", especially in the context of this type of AI-enabled technology, and the information it collects.

[65] Contrary to the University's statement, its collection of personal information in the context of online proctoring remains subject to the necessity requirement of s. 38(2). The university has statutory obligations to its students relating to the collection, use, privacy, and security of the personal information it collects and must demonstrate it is fulfilling them, regardless of any administrative efficiency or commercial advantage of any particular software.

[66] While online proctoring software must collect personal information to perform its exam proctoring function, it remains that Respondus Monitor collects particularly sensitive information. This includes biometric information and can also include background images or sounds that may provide information about the student they may not wish to share and raises risks of unfair allegations or decisions being made about them based on inaccurate information. These risks must be appropriately mitigated by effective guardrails that the university should have in place to govern its adoption and use of such technologies. In the absence of legislation regulating the use of AI in Ontario, I go on to outline what I believe some of those guardrails should be in the final section of this decision, entitled "Other Recommendations".

Issue 3: Is the notice of collection in accordance with section 39(2) of the *Act*?

[67] Under the *Act,* an institution is required to provide individuals with formal notice of the collection of their personal information. The purposes of the notice are to ensure that the institution's practices with respect to personal information are transparent and that the institution is accountable to the individual. Section 39(2) of the *Act* imposes the following notice requirement on institutions that collect personal information:

> (2) Where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of,
>
> (a) the legal authority for the collection;
>
> (b) the principal purpose or purposes for which the personal information is intended to be used; and
>
> (c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

[68] McMaster provided a Statement on Collection of Personal Information and Protection of Privacy[16] (the Notice Statement), available online, which states that it

[16] https://pgme.mcmaster.ca/app/uploads/2023/02/FIPPA_Statement.pdf

collects personal information of students under the authority of the *McMaster University Act, 1976*, in accordance with section 39(2)(a).

[69] The Notice Statement sets out a number of uses for this information, including use for academic and administrative purposes. It directs those with questions regarding collection and use of personal information to the University Registrar or University Secretary. In addition to the Notice Statement, the university has furnished other online resources that provide information about Respondus, including "An Introduction to Respondus"[17] and "FAQs on Respondus Online Proctoring" aimed at students.[18]

[70] Through these various documents, the university provides students with useful information about Respondus. However, as it now stands, students must search for and consult a number of disparate web pages to discover all the relevant information. Given the sensitivity of the information collected, I find that the spirit and intent of the notice requirement set out in 39(2)(b) of the *Act* is not satisfied by requiring students to consult multiple sources to see the totality of purposes for which their personal information is to be used. I recommend therefore that the university consolidate its notice of collection of personal information via Respondus Monitor in a clear and comprehensive statement, either in a single source document, or with clear cross-references to other related documents, so that students can access this information in a coherent, plain language and accessible way, without having to navigate through a number of other online sources.

[71] The final requirement under section 39(2)(c) is the need to provide the title, business address, and business telephone number of officials to whom questions regarding collection may be directed. Earlier during this investigation, the university stated that the University Registrar or University Secretary could be contacted about general privacy concerns but did not provide a business telephone number for those individuals in compliance with section 39(2)(c). In response to my office's concerns about this, the university has since addressed the issue by including the name, title, email, and business telephone number of the designated contact person(s) in its online collection notice, satisfying the requirement of section 39(2)(c).[19]

Issue 4: Was the use of personal information in accordance with section 41(1) of the *Act*?

[72] Section 41(1) of the *Act* limits the use of personal information as follows (in part):

> (1) An institution shall not use personal information in its custody or under its control except,

[17] https://mi.mcmaster.ca/app/uploads/2021/03/An-Introduction-to-Respondus-_updated.pdf
[18] https://studentsuccess.mcmaster.ca/respondus-online-proctoring/
[19] The university's revised collection notice is now titled "Notice of Collection, Use and Disclosure Statement" and is available at https://secretariat.mcmaster.ca/privacy/notice-of-collection-use-and-disclosure/

> (a) where the person to whom the information relates has identified that information in particular and consented to its use;
>
> (b) for the purpose for which it was obtained or compiled or for a consistent purpose; …

[73] A "consistent purpose" is explained in section 43 as follows:

> Where personal information has been collected directly from the individual to whom the information relates, the purpose of a use or disclosure of that information is a consistent purpose under clauses 41 (1) (b) and 42 (1) (c) only if the individual might reasonably have expected such a use or disclosure.

[74] Due to the nature of its function, Respondus Lockdown Browser captures limited personal information necessary for the purpose of exam administration. I have already determined that the collection of personal information via Respondus Lockdown Browser for that purpose is authorized under the *Act*. I find therefore that the use of that information for the same purpose is also authorized pursuant to section 41(1) of the *Act*.

[75] In contrast, Respondus Monitor captures much more personal information. It analyzes audio and video footage of a student, using their biometric data and other inputs to assess whether a student's exam session should be flagged to the instructor as a possible academic integrity issue. This personal information is compared with baseline data for all videos analyzed by Respondus Monitor, and with data from other test takers of the same exam. Respondus then weighs the various elements and provides other adjustments before communicating the review priority of the exam session to the instructor.

[76] As I have found, Respondus Monitor collects students' personal information on behalf of the university for its lawfully authorized purpose of proctoring examinations. I also find that it uses the personal information for that same purpose. However, I must go on to consider whether the personal information collected by Respondus Monitor is being used for any other purposes.

[77] From the information provided, it is clear that Respondus uses at least some data gathered from test takers to improve its own services.

[78] In its online information about its products, Respondus describes its own use of student information as follows:

> Respondus personnel do not review/analyze the recordings except as may be required to resolve technical problems, improve system performance,

> modify Respondus Monitor, investigate violations of these Terms, or as may be directed by your Institution or applicable law enforcement.[20]

[79] The Respondus Monitor Terms of Use provides further details on the type of information it may use to improve its system, and how it does so:

> Random samples of video and/or audio recordings may be collected via Respondus Monitor and used by Respondus to improve the Respondus Monitor capabilities for institutions and students. The recordings may be shared with researchers under contract with Respondus to assist in such research. The researchers are consultants or contractors to Respondus and are under written obligation to maintain the video and/or audio recordings in confidence and under terms at least as strict as these Terms. The written agreements with the researchers also expressly limit their access and use of the data to work being done for Respondus and the researchers do not have the right to use the data for any other purposes. No personally identifiable information for students is provided with the video and/or audio recordings to researchers, such as the student's name, course name, institution, grades, or student identification photos submitted as part of the Respondus Monitor exam session.[21]

[80] Respondus states that the random samples of recordings, either audio or video, are not associated with any other direct identifiers that would lead to the student being identifiable. McMaster also describes this as a use of anonymized data, rather than personal information, stating that:

> Respondus does collect anonymized, aggregated data on the use of its service to help improve performance, diagnose problems, and detect and prevent fraud and abuse of its services and systems.[22]

[81] However, McMaster has already agreed, and I have found, that the video recordings of students are personal information. Further, this office has also previously determined that recordings of an individual contain their personal information.[23]

[82] Use of personal information for improvement of Respondus' services is clearly not the same purpose for which it was collected, namely to proctor examinations on behalf of the university, nor do I find that it is a consistent purpose. Section 43 of the *Act* stipulates that use of personal information may only be considered to be consistent with the purpose for which it was collected if "the individual might reasonably have expected such a use."

---

[20] https://web.respondus.com/privacy/privacy-additional-monitor/
[21] https://web.respondus.com/tou-monitor-student/
[22] https://studentsuccess.mcmaster.ca/respondus-online-proctoring/
[23] See Privacy Complaint Report MC07-68, among others.

[83] In my view, students would reasonably expect that their university would follow best practices when dealing with their personal information, limit the use of their personal information to that which is necessary to conduct exams with integrity, and not allow third party vendors to use their personal information for purposes unrelated to their education without their consent.

[84] Students would not reasonably expect that the university, having collected their personal information via Respondus to proctor exams, would permit Respondus to then use that personal information to advance the company's own commercial purposes.

[85] A review of the relevant documents did not identify any ability for students using Respondus Monitor either to consent to, or opt out of, having their video or audio recordings used by Respondus for improvement of its system performance or capabilities.

[86] I find therefore that the use of student audio and video recordings for the purpose of improving Respondus Monitor's system performance or capabilities is not authorized under section 41(1) of the *Act*.

[87] From publicly available information about its services, it appears that Respondus is able to provide Respondus Monitor exam proctoring services without using the personal information in the student recordings for the purposes of improving its services.

[88] Respondus has stated publicly that in some jurisdictions, it does not use personal information to improve its product. In "Algorithmic Fairness and Respondus Monitor Proctoring: A study using Casual Conversations,"[24] authored by Respondus' CEO and its Chief Scientist, they note that "[no] data from the European Union, California, and certain other regions are used for research or product improvement purposes." This is consistent with information available on the Respondus' website, which includes separate sections for the privacy protections provided to residents of the EU and California.

[89] Given this apparent ability, I recommend that McMaster secure the written undertaking from Respondus that it will respect Ontario law by ceasing to use students' personal information for system improvement purposes without the consent of students. If such an undertaking is not promptly provided and acted upon, I recommend that McMaster cease the use of Respondus Monitor until such time as it enters into a new particularized agreement with Respondus containing these restrictions, as well as the other provisions recommended below.

Issue 5: Does the university have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students, in accordance with the requirements set out in

[24] Available at https://web.respondus.com/wp-content/uploads/2022/04/Algorithm_Fairness_4.7.22.pdf

section 4(1) of Ontario Regulation 460 and sections 4(1) and 5 of Ontario Regulation 459, made pursuant to the *Act*?

[90] When an institution contracts with a third party to provide information management functions, the institution's obligations to comply with *FIPPA* continue. As such, there must be contractual and oversight measures in place to ensure that the institution remains in compliance with the *Act*.[25]

[91] McMaster has contracted with Respondus to provide exam proctoring services. Under the *Act*, the university remains responsible for the security, retention and destruction of personal information in its custody or control.

[92] Ontario Regulation 460, made pursuant to the *Act*, establishes rules for the security and retention of records in the custody of an institution. Section 4(1) of that regulation requires that institutions define, document, and put in place measures that are reasonable to prevent unauthorized access to the records in their custody or control, including records containing personal information. Ontario Regulation 459 under the *Act* sets out specific rules governing the secure disposal and destruction of personal information.

[93] Each institution is different and may devise its own approach to meeting the requirements in Regulation 460. As noted by Investigator Lucy Costa in Privacy Complaint Report PR16-40, the regulation does not prescribe a "one-size-fits-all" approach to security:

> It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions. [26]

[94] Where an institution subject to the *Act* retains a private sector entity to provide core functions on its behalf, it must take all reasonable and appropriate measures to ensure that the entity deals with the records under the control of the institution in ways that comply with the institution's obligations under the *Act*. The principal means by which the institution may achieve this objective is through provisions in its contract with the private sector entity that ensure the services performed on the institution's behalf comply with the rules and safeguards set out in the *Act*.[27]

---

[25] Ontario Criminal Code Review Board [1999] O.J. No. 4072 (C.A.) and Privacy Complaint Report PR16-40.
[26] Privacy Complaint PR16-40 at para 72.
[27] Ibid. at paras 116-117.

Contractual and Business Relationship

[95] Respondus and McMaster signed a "LockDown Browser License Agreement for Non-Profit Educational Institutions" (License Agreement) for the 2020-21 school year, which has since been renewed. The License Agreement is largely focussed on the rights conferred on McMaster to use Respondus' software, and the monetary cost associated with this. The License Agreement lists the "Software Product" as LockDown Browser, and refers to Respondus Monitor as an "optional, companion service" that the Licensee "can enable or disable … during the License Term, subject to a separate Terms of Use agreement." The annual fees listed in the License Agreement include amounts specific to both LockDown Browser and Monitor, with Monitor usage forming the bulk of the associated cost.

[96] McMaster did not provide any separate agreement or contract specific to Respondus Monitor. However, it appears that Respondus has general terms in place for institutions that do not enter into a particularized agreement with Respondus regarding the use of Monitor.

[97] On its website, Respondus publishes a document titled "Terms of Use – Respondus Monitor (Institution)" (Monitor TOU)[28]. The preamble to this document states that it is provided for reference, that terms may vary by region, and "[c]ertain institutions may also use customized versions of these terms." The Monitor TOU states that it is an agreement between the institution and Respondus "regarding the Institution's use of Respondus Monitor," specifying that the institution "agrees to these Terms in full before using Respondus Monitor."

[98] McMaster has been using and paying for the use of Respondus Monitor since 2020. According to the Monitor TOU, once it started using this service, the Monitor TOU came into effect. Given this, and in the absence of a separate agreement between Respondus and McMaster regarding Respondus Monitor, the provisions in the Monitor TOU apply between McMaster and Respondus.

[99] Respondus also publishes the following privacy-specific information regarding its products:

- Data Processing Agreement[29]
- Respondus Product Privacy Policy (Privacy Policy)
- Additional Privacy Information – Respondus Monitor (Monitor Privacy Information)

[28] https://web.respondus.com/tou-monitor-admin/
[29] https://web.respondus.com/data-processing/.

- Additional Privacy Information – LockDown Browser (LockDown Privacy Information)

[100] The License Agreement does not substantively address privacy or security matters but is specifically linked to the Privacy Policy. Further, the Data Processing Agreement states in its preamble that it forms part of the License Agreement. The Monitor TOU states that it incorporates by reference both the Privacy Policy and the Data Processing Agreement. There is no mention of the Monitor Privacy Information or the LockDown Privacy Information being incorporated by reference or otherwise forming part of the contractual agreement.

[101] In Privacy Complaint Report PR16-40, Investigator Costa enumerated the contractual provisions that may be relevant in assessing whether the institution in that matter had discharged its obligations to ensure that all reasonable steps were taken to protect the privacy and security of personal information under its control. These included provisions relating to:

- Ownership of Data
- Confidential Information
- Collection, Use and Disclosure
- Notice of Compelled Disclosure
- Subcontracting
- Security
- Audits
- Retention and Destruction

[102] I adopt this assessment framework and address below the adequacy of McMaster's contractual and oversight measures governing its relationship with Respondus.

Ownership

[103] The Data Processing Agreement describes Respondus as a "processor" of personal information, stating that the licensing institution "maintains ownership and controls all access to the Licensee data in its account." The Data Processing Agreement also states that Respondus will not access any Licensee Data except as necessary for the operation of the services or as expressly permitted by the Licensee, unless otherwise required by law to do so.

[104] In addition, the Monitor TOU states that "Respondus does not claim ownership in the information or data [the institution] or any students provide". The Monitor TOU goes

on to state that Respondus has a license to "use, store, modify, copy, and transmit any such information or data" but limits the purposes of doing so to the carrying out of services in accordance with the Monitor TOU.

[105] Based on the above, I am satisfied that McMaster retains ownership of the information held by Respondus.

Confidential Information

[106] Respondus uses the term "personal data" which it defines in the Data Processing Agreement as having the meaning set out in the applicable data protection law. "Personal data" under the Data Processing Agreement therefore incorporates the definition of "personal information" found in s. 2 of the *Act*.

[107] The Privacy Policy, incorporated by reference into the Monitor TOU, also provides the following definition:

> Personal data is a name, address, telephone number, email address, identification number, online identifier, or other data collected that could directly or indirectly identify you. This is also known as Personal Information or Personally Identifiable Information (PII).

[108] The Privacy Policy describes Respondus' use of personal data generally as follows:

> We strongly believe in both minimizing the personal data we collect and limiting its use and purpose to only: (1) that for which we have been given permission, (2) that which is necessary to deliver the products you purchase or interact with, or (3) as we might be required or permitted for legal compliance or other lawful purposes.

[109] The Privacy Policy differentiates between aggregate data and information that is either personal data or may be linked to personal data, as follows:

> Much of the data collected is aggregated or statistical data about how individuals use our Services, but to the extent that product data is itself personal data, or is linked or linkable to personal data, we treat it accordingly.

[110] The Data Processing Agreement states that Respondus may "de-identify Licensee Data … and may process De-Identified Data to maintain and improve the services."

[111] Taken together, the provisions in the Data Processing Agreement and the Monitor TOU (including the incorporated Privacy Policy) do not provide adequate protections for the personal information contained in video and audio recordings.

[112] Respondus uses samples of video and audio recordings to improve its services,

stating that these samples do not have any *other* identifying information associated with them[30] and appears to treat them as de-identified data. However, I have already found that video and audio recordings of individual students can be used to identify the student and that such recordings constitute the student's personal information whether or not they are associated with other identifiers.

[113] Given this, I am not satisfied that Respondus affords to these sample recordings the same confidentiality protections afforded to other personal information. I recommend therefore that McMaster seek confirmation from Respondus that it will treat and protect all audio and video recordings, regardless of length, and any inferences or information related thereto, as personal data.

Collection, Use, and Disclosure

[114] The Monitor Privacy Information states that during exams, Respondus creates a facial template to determine if the student who started the exam differs from the person in the video frame throughout the duration of the exam.[31] It also states that the template is not saved on the student's computer or to the cloud server database, and it is cleared from the computer immediately after exam completion, and from the server's memory no later than two days after exam completion. It appears from the foregoing that Respondus has undertaken to collect no more facial detection information than is necessary for functional purposes, that its use is limited to those purposes, and that the facial data collected is deleted after a reasonably short period of time.

[115] As outlined above, the Data Processing Agreement limits Respondus' access to the Licensee Data to what is necessary for the operation of the services, expressly permitted by the Licensee, or required by law. The Privacy Policy outlines similar restrictions and states that Respondus minimizes the personal data it collects.

[116] As noted above, however, Respondus appears to regard the video and audio recordings as de-identified data that may be used to maintain or improve its services and system performance. This is confirmed by the Monitor TOU which states that Respondus uses video and/or audio recordings to improve Respondus Monitor's capabilities, and that this may include sharing these recordings with researchers under contract with Respondus without providing them with any personally identifying information.

[117] For the reasons outlined above, I am not satisfied that the Data Processing Agreement, Monitor TOU, and Privacy Policy provide adequate protection for the collection, use, and disclosure of the personal information in the video and audio recordings. To address this, I reiterate my recommendation that McMaster secure a written undertaking from Respondus that it will cease the use of students' personal information for research or product improvement purposes without the consent of

---

[30] See "Privacy and Security Policy" section of Monitor TOU, available at https://web.respondus.com/tou-monitor- admin/

[31] https://web.respondus.com/privacy/privacy-additional-monitor/

students.

Notice of Compelled Disclosure

[118] The Privacy Policy addresses the circumstances in which Respondus may disclose personal information to authorities, stating:

> Respondus does not voluntarily or actively transfer or disclose our customers' personal data to government or law enforcement authorities. In the event of a request from a government or law enforcement authority, we have procedures and controls in place to make sure that such a request is assessed and challenged to confirm its validity.

[119] The Monitor TOU states that Respondus "reserves the right at all times to disclose any information or data (including recordings and any content to the extent applicable) … to comply with the law."

[120] After reviewing the relevant documents, I was not able to find any requirement that Respondus notify the Licensee in the event that it is required to disclose a user's personal data to authorities. An institution should require service providers to provide it with prompt notice of any such compelled disclosure of personal information to government or law enforcement to allow it to seek an appropriate remedy to prevent or limit such disclosure. Further, the institution should require the service provider to disclose only the personal information it is legally compelled to disclose. Accordingly, I recommend that McMaster should secure a written undertaking from Respondus incorporating the above-noted requirements.

Subcontracting

[121] The Data Processing Agreement states that any person authorized to process Licensee Data, including subcontractors, shall be subject to a "legally-binding duty of confidentiality" and that Respondus shall ensure that authorized persons, including subcontractors, shall maintain the security of this data and process it only as necessary for operation of the services or as expressly permitted by the Licensee.

[122] The Data Processing Agreement permits subprocessing, as Respondus' servers are operated by a third-party hosting provider, that is a subprocessor under applicable data protection law. This agreement states that the Licensee consents to the appointment of this subprocessor but notes that "Respondus shall impose data protection terms that are consistent with the terms of this DPA and the Applicable Data Protection Laws." The Data Processing Agreement further specifies that "Respondus remains fully liable for any breach of this DPA by any act, error or omission of its Subprocessor."

[123] However, as noted above, the Monitor TOU also contemplate subcontracting research on the use of sample recordings to maintain or improve Respondus Monitor services. I have already determined that this does not provide adequate protection of

students' personal information. I reiterate my recommendation that McMaster seek an express undertaking or include provisions in a particularized Respondus Monitor Terms of Use Agreement prohibiting the use or disclosure of personal information, including video or audio recordings, for the purpose of improving Respondus' system or similar purposes.

Security

[124] The Data Processing Agreement addresses security measures as follows:

> Respondus shall implement appropriate technical and organizational measures to protect the Licensee Data from unlawful processing and/or a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the nature, likelihood and severity of the risk to the rights and freedoms of natural persons.

[125] The Data Processing Agreement goes on to set out the measures it shall take, as appropriate, as part of the security protections, including the encryption of personal data, the ability to restore and access personal data in a timely manner if an incident occurs, and a process for regularly testing and evaluating the effectiveness of the measures in place.

[126] The Respondus Data Processing Agreement also requires Respondus to notify Licensees in the event of a breach, stating as follows:

> If Respondus becomes aware of an actual Security Incident[32] that involves Licensee Data, Respondus will: (a) notify Licensee of the Security Incident without undue delay; (b) take appropriate steps to identify the cause of the Security Incident, minimize harm and secure the Licensee Data; and (c) provide Licensee with information as may be reasonably necessary to assist Licensee with its notification and reporting responsibilities.

Audits

[127] The Data Processing Agreement provides Licensees with the right, once a year, to submit audit questions relating to Respondus' processing and protection of data. Respondus is required to respond to those questions. It is also required to "maintain complete and accurate records and information to demonstrate its compliance with [the Data Processing Agreement]" and make these records available for audit by its Licensees.

---

[32] The Data Processing Agreement defines "security incident" as a personal data breach under the European Union's General Data Protection Regulation.

Retention and Destruction

[128] The Data Processing Agreement states that Respondus will retain Licensee Data for the period of time described in the License Agreement and Monitor TOU and elaborates on the deletion of data as follows:

> Upon termination of the Licensee's elected data retention period, or upon request of the Licensee, Respondus shall delete all Personal Data processed on behalf of the Licensee, unless a further period of time is provided for the storage of Personal Data under a provision of Applicable Data Protection Law. Upon request, Respondus shall provide a written statement confirming the deletion of the Licensee Data along with the deletion of all existing copies of the Licensee Data, within and no later than 7 (seven) days from the deletion of the Licensee Data.

[129] In addition to the overall retention policy described in the Data Processing Agreement, the Monitor Privacy Information states that the "temporary template of facial identifiers" used during an exam session is not saved to the cloud server's database or storage and is cleared from the server's memory no later than two days after the exam is completed.

[130] As for the audio and video recordings captured through Respondus Monitor, these are created during exams for the purposes of ensuring that students are not cheating in that course. Therefore, any possible utility of the recordings would reasonably end with the conclusion of the course term. I recognize that McMaster operates several different academic terms, and that some courses are multi-term courses. Given this, I recommend that McMaster contractually require Respondus to delete McMaster's data from its servers on, at minimum, an annual basis, unless McMaster requests otherwise, and that Respondus provide confirmation of this deletion.

[131] In specific cases that lead to academic integrity investigations requiring the review of audio and video recordings captured through Respondus Monitor, the university states that such recordings would be subject to the records retention policy for academic integrity investigations.

[132] In respect of Respondus Lockdown Browser, McMaster stated in its PIA Summary that students could remove the software after the exam has concluded and it is no longer necessary. McMaster acknowledged to my office that it had not looked into whether this removal entirely wiped the Respondus software from student computers. I recommend that McMaster conduct tests to confirm that uninstalling Respondus after an exam actually results in the removal of the totality of that software, with no remnants of it remaining on the computer.

Other Recommendations

[133] McMaster has adopted a tool that employs artificial intelligence technology to

automate proctoring exams online and help inform inferences or decisions about academic integrity that can have significant impacts on its students.

[134] My analysis and recommendations above pertain to McMaster's current statutory obligations to protect students' personal information under the *Act*. Although there is no current law or binding policy specifically governing the use of artificial intelligence in Ontario's public sector, I recommend that McMaster build in additional guardrails to protect its students from the heightened risks associated with its AI-enabled proctoring software.

[135] Together with my counterparts across Canada[33] I have called for strong guardrails to ensure AI systems, including generative AI, are safe, privacy protective, transparent, accountable, and human rights affirming.

[136] The Government of Ontario has acknowledged the need to develop guardrails for the use of artificial intelligence technology in the public sector and is in the process of developing Ontario's Trustworthy Artificial Intelligence (AI) Framework.[34]

[137] In a joint statement I issued with the Chief Commissioner of the Ontario Human Rights Commission[35], we urged the government to press forward with finalizing its Trustworthy AI framework into a binding set of robust and granular rules that effectively address safety, privacy, accountability, transparency, and human rights. We set out our rationale in the Joint Statement as follows:

> AI technologies have great potential to benefit society in terms of improved health, education, public safety, and social and economic prosperity. However, they have also been shown to be unsafe when not effectively governed. They often rely on immense volumes of personal information, which may not be properly protected, and the initial collection of this information may not always be lawful. Even where information has been de-identified, AI technologies can perpetuate biases and lead to disparate impacts on Ontarians. This is particularly true for historically marginalized individuals or groups, including those protected under human rights legislation.
>
> AI technologies can support the drawing of inferences and decision-making processes that are opaque or difficult to understand or challenge. The use of AI technologies, especially generative AI systems, may create flawed or inaccurate content that raises concerns about how government can ensure

---

[33] Principles for responsible, trustworthy and privacy-protective generative AI technologies, December 7, 2023, https://priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/

[34] https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework

[35] Joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies, May 25, 2023, online: https://www.ipc.on.ca/?post_type=news-release&p=21033

> accountability for their use. All of those risks are compounded where AI technologies are not adequately evaluated before and after their adoption, including the risks of ingraining or amplifying historical systemic biases or discriminatory practices. The harms presented by those risks can be more damaging without meaningful engagement with potentially affected parties about whether to develop, acquire, or deploy these technologies, including what rules should govern their use.

[138] I acknowledge that the university has already carried out a level of due diligence prior to adopting Respondus Monitor, including carrying out a pilot project, completing a PIA, examining the vendor's policies, protocols and terms of use, and developing its own policies and related communication materials, such as FAQs for both teachers and students on how the AI software works. However, given the significant risks and potential harms associated with AI tools that can adversely impact students' rights, I recommend that McMaster go further by adopting additional guardrails, including the following.

PIA and Algorithmic impact assessment

[139] Given the broad range of privacy and human rights and impacts at stake with AI, I recommend that McMaster undertake an algorithmic impact assessment (AIA)[36] in addition to its PIA. An AIA is an additional tool that contains a series of questions and prompts to help organizations assess the potential impacts of an automated decision-system.

[140] An AIA will help assess the level of risks associated with the university's use of Respondus Monitor for the purpose of proctoring online exams, conduct a higher level of scrutiny over the source or provenance of the data used to train its algorithms, and consider the potential impacts it can have not only on the rights of individual students, but on the interests of broader communities of students on campus and the overall level of public trust in the university. Most importantly an AIA can help the university identify and focus on concrete ways of mitigating some of these risks and potential impacts.

[141] In its response to an earlier version of this report, the university has committed to using the Treasury Board of Canada's tool to conduct AIAs as part of its privacy impact assessments. This is particularly important until such time as Ontario develops a similar tool for its public and broader public sectors.

Consultation with affected communities

[142] Ideally, institutions considering adopting AI technologies should meaningfully engage and consult with affected parties and those with relevant expertise prior to adoption, and on a regular basis thereafter. This consultation is critical for understanding

---

[36] For example, see Treasury Board of Canada's Algorithmic Impact Assessment tool available at: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html

the full scope of potential issues that may arise, and how these issues may impact, be perceived, and be experienced by others.

[143] Being attentive to these considerations from the start and throughout implementation allows the institution to be alert to issues that may arise, respond quickly to change its approach mid-course, and if need be, reassess whether to proceed with using the technology, or move towards a different approach less prone to such pitfalls.

[144] I recommend that McMaster carry out this necessary consultation step with representatives of its many diverse communities among its student population, particularly those from vulnerable or historically marginalized groups. These consultations should also include necessary experts in privacy and human rights, as well as technologists with relevant expertise to understand how the underlying algorithms work and their potential adverse or differential impacts on communities.

Broader opportunity for students to opt-out

[145] It is a known fact that AI technologies are not necessarily neutral or accurate. Bias within an algorithm may have the unintended effect of reinforcing discrimination towards vulnerable and historically marginalized communities or arriving at decisions that are individually or systematically unfair or unjust.

[146] For example, the video component of automated exam proctoring may result in certain individuals or groups being treated differently. Some research suggests that individuals with darker skin tones are flagged more often.[37] Others have noted that the students with certain disabilities may involuntarily move or speak in a way that would also lead to additional flagging and potentially false positives.[38]

[147] In McMaster's case, students with disabilities are accommodated by using live invigilation, rather than automated proctoring through Respondus Monitor. However, AI-powered technologies may potentially trigger other protected grounds under human rights that require similar accommodations, such as color, race or ethnic origin.

[148] It is not within my mandate to make findings or recommendations under human rights law. However, I encourage McMaster to make special arrangements not only for students requesting formal accommodation under a protected ground in human rights legislation, but also for any other students having serious apprehensions about the AI-enabled software and the significant impacts it can have on them and their personal information. Now that in-person invigilation is possible post COVID, all students should

---

[37] Racial, skin tone, and sex disparities in automated proctoring software, Frontiers in Education, September 2022, available at https://doi.org/10.3389/feduc.2022.881449. Respondus' own publication, "Algorithm Fairness and Respondus Monitor Proctoring: A study using Casual Conversations" also found an increased error rate in poor lighting conditions for the darkest skin tone classification.

[38] How Automated Test Proctoring Software Discriminates Against Disabled Students, Lydia X. Z. Brown, November 16, 2020, available at https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/

be provided with the general opportunity to opt out of online exam proctoring in favor of in-person exams depending on their personal circumstances and general level of comfort with this relatively invasive technology.

Human Supervision and ability to challenge results

[149] Institutions remain ultimately responsible for ensuring the accuracy of the data they use and the validity of decisions they make based on information the AI tool provides, infers or generates.

[150] McMaster has built in an appropriate level of human oversight over Respondus Monitor by ensuring that any flags detected by the software are brought to the attention of the instructor. The instructor is to review the flag and begin a conversation with the student if there is a concern. The instructor can only review the video upon request and as appropriate, and only then can a charge be brought under the Academic Integrity Policy and a potential investigation into potential academic misconduct ensue.

[151] In its student FAQs on Respondus Online Proctoring, under the section entitled "What if…?", McMaster tells its students "not to worry" and "don't panic" if the system happens to flag their movements or their conduct as suspicious, explaining that their instructor will conduct a review of the recording. "This means it will be up to a human, and not a computer, which cases are investigated further."

[152] The FAQs go on to describe possible scenarios that might occur, and suggest how students may try to avoid them, or if they do happen, how students can explain them during the exam, or immediately thereafter, and to whom.

[153] The FAQs later explain that the audio and video recordings taken of students, as well as any additional information about the student's computer use during the exam, will be assessed by the instructor to determine whether a flagged case requires further follow up, including referral as a possible breach of McMaster's Academic Integrity Policy.

[154] However, the FAQs are silent in terms of explaining how students can challenge allegations or inferences made about them by the instructor, based on flags identified by the proctoring software. Presumably, at that point, the full weight of the university's academic integrity policy comes to bear on the rights and obligations of the parties, including the student's right to a hearing.

[155] However, given the fallibility of many AI tools, I recommend that McMaster provide a less formal means for students to challenge flags identified by the Respondus Monitor software, including their instructor's subsequent review, prior to invoking the formal academic integrity process that can be a very heavy one. Students should be provided with a meaningful opportunity to explain their situation. Where warranted, students should have the right to correct the information, and have the flag removed and any inferences or allegations based on the flag deleted from their student record. It is possible that McMaster already provides students with this informal opportunity to explain in

practice. However, I recommend that its FAQs aimed at students provide explicitly for the possibility of this informal step and communicate it in a way that is understandable and actionable for its intended audience.

Use of vendors

[156] Institutions choosing to use AI technologies must remember that these tools are working for them, and pursuant to their statutory authorities and obligations. While they can outsource their data processing functions, they cannot outsource they responsibility. Ultimately, the institution should not satisfy itself with AI technology that operates in a "black box", without being able to understand and explain how the technology functions.

[157] Organizations should ensure that the vendor of any AI tool selected has designed its tool in a manner that ensures safe and accurate results, accounts for heightened privacy and security concerns which may be associated with AI technology, and mitigates against any potential bias and discriminatory impacts.

[158] In its online FAQs, McMaster assures its students that it has conducted an in-depth review of Respondus' data security and privacy practices in the context of its PIA. This includes having reviewed the company's publicly available material such as its privacy policy and terms of use, as well as its internal policies and protocols for greater detail on its collection, use, access and disclosure of personal information, and its security safeguards and incident management protocols.

[159] However, it is not clear whether McMaster has enquired into other aspects of Respondus Monitoring software, such as how the algorithm works and the provenance of the data used to train the system.

[160] As a private sector organization, Respondus falls outside my office's jurisdiction and a full review of the company's operations is beyond the scope of my mandate.

[161] However, as explained above, McMaster remains accountable for the protection of its students' privacy rights and any decisions it makes based on the personal data it collects about them, even when it outsources data processing capabilities, including AI, to third party vendors.

[162] The use of AI technologies in exam proctoring is not particular to Respondus, as there are other competitors who provide similar services[39]. However, if McMaster is contemplating continuing its business relationship with Respondus and decides to enter into a particularized agreement in respect of the Respondus Monitor software, the university should conduct greater scrutiny over how this tool was developed and how it

[39] See, for example, "Examity Launches AI Enabled Proctoring Solution at UC Davis" available at https://www.examity.com/examity-launches-ai-enabled-proctoring-solution-at-uc-davis/ and "Paving the Way for Ethical Technology" available at https://proctorio.com/about/blog/paving-the-way-for-ethical-technology .

is used.

[163] Specifically, this means that in addition to the provisions I recommend McMaster include in its agreement with Respondus outlined above, I recommend that the university also ensure that any data used by Respondus to train its algorithms was obtained in compliance with Canadian laws, and in keeping with Ontarians' reasonable expectations of privacy.

[164] Furthermore, I recommend that in its negotiation for a particularized agreement for the use of Respondus Monitor, McMaster should prohibit the use of its students' personal information for algorithmic training purposes, unless the company can demonstrate a process for obtaining their meaningful consent.

[165] On a broader level, McMaster remains accountable for the continued use of AI technologies throughout their lifecycle and across the variety of circumstances in which they are used. This includes continually evaluating the reliability of the tool. Even once a particularized agreement is in place for the use of Respondus Monitor, McMaster should continue to monitor for and alert Respondus to potential inappropriate uses or biased outcomes that may not have been disclosed as a potential limitation of their system. Conversely, McMaster should require Respondus to also monitor for, and inform the university of any weaknesses, biases or vulnerabilities it discovers about the program.

[166] The adoption and application of the above guardrails would allow institutions such as McMaster to make responsible use of AI technologies to help carry out its lawfully authorized activities, while protecting against discriminatory impacts and promoting students' privacy. I acknowledge that several of McMaster's practices already demonstrate an understanding of the heightened need to protect the privacy rights of students when utilizing these types of technologies. However, to the extent there may be gaps, I recommend McMaster adopt the additional guardrails above and build them into its online proctoring program and/or its contractual provisions with Respondus as appropriate.

CONCLUSION:

1. The students' names, course information, biometric data, photo identification, and audio and video recordings are "personal information" as defined in section 2(1) of the *Act*.

2. The collection of personal information via Respondus LockDown Browser and Respondus Monitor is in compliance with section 38 of the *Act*.

3. The university's notice of collection does not comply with 39(2) of the *Act*.

4. The use of personal information via Respondus LockDown Browser on behalf of the university is authorized under section 41(1) of the *Act*, but the use of personal

information via Respondus Monitor for product improvement purposes is not in compliance with section 41(1) of the *Act*.

5. The contractual and oversight measures in place are not sufficient to ensure the privacy and security of the personal information of its students, in accordance with the requirements of section 4(1) of Ontario Regulation 460 and sections 4(1) and 5 of Ontario Regulation 459 made pursuant to the *Act*.

RECOMMENDATIONS:

1. The university should consolidate its notice of collection of personal information via Respondus Monitor in a clear and comprehensive statement, either in a single source document, or with clear cross- references to other related documents, so that students can access this information in a coherent, plain language and accessible way, without having to navigate through a number of other online sources.

2. The university should secure a written undertaking from Respondus that it will cease using students' personal information for service improvement purposes and disclosing students' personal information to subcontractors for research purposes, without the consent of students. If Respondus does not promptly provide and act upon such an undertaking, I recommend that McMaster cease the use of Respondus Monitor until such time as it enters into a particularized agreement with Respondus containing these and other restrictions, recommended below.

3. The university should seek confirmation from Respondus that it will treat and protect all audio and video recordings, regardless of length, and any inferences or information related thereto, as personal data.

4. The university should secure a written undertaking from Respondus that in cases of compelled disclosure of personal information to government or law enforcement, it will provide McMaster with prompt notice of any such compelled disclosure to allow it to seek an appropriate remedy to prevent or limit such disclosure. Further, the written undertaking should require Respondus to disclose only the personal information it is legally compelled to disclose.

5. The university should contractually require that Respondus delete personal data from its servers on an annual basis, minimally, and that it provide the university with confirmation of data deletion when it occurs.

6. The university should conduct tests to confirm that uninstalling Respondus LockDown Browser actually results in the removal of the totality of that software, with no remnants of it remaining on the computer.

7. The university should adopt additional guardrails for the heightened privacy risks associated with the use of its AI-enabled exam proctoring software in its program and policies, and in its contractual relationship with Respondus where appropriate. These include guardrails to:

    a. conduct an algorithmic impact assessment, in addition to a PIA;

    b. carry out consultation with representatives of its many diverse communities among its student population, particularly those from vulnerable or historically marginalized groups;

    c. provide students with an opportunity to opt out of online proctoring, and choose in person invigilation instead;

    d. provide a less formal means for students to challenge flags identified by the Respondus Monitoring software prior to invoking the formal academic integrity process, and inform students more explicitly of this possibility;

    e. Conduct greater scrutiny over how the Respondus Monitoring software was developed to ensure that any source data used to train its algorithms was obtained in compliance with Canadian laws and in keeping with Ontarians' reasonable expectations;

    f. Prohibit Respondus from using students' personal information for algorithmic training purposes without their consent; and,

    g. Continue to monitor for, and document, any inappropriate uses or biased outcomes that may not have been disclosed as a potential risk of limitation of the software and inform the vendor accordingly, and require Respondus to do and inform it of same.

Within six months of receiving this Report, the university should report back to my office regarding the implementation of these recommendations.

Patricia Kosseim
Commissioner

February 28, 2024