# Respondus Concerns

*2020-09-24*

To whom it may concern,

Many instructors compel the usage of Respondus software for students to write their exams. I am not comfortable with how this software intrudes upon my privacy. I have reached out to my professors individually in an attempt to find a mutually satisfactory resolution, however not all of my concerns were addressed.

For those who are unfamiliar with Respondus's software offerings, here is a brief quote from Respondus[1] that describes how their product—*Respondus Monitor*—functions:

> At the heart of Respondus Monitor is a powerful artificial intelligence engine, Monitor AI, that performs a second-by-second analysis of the exam session. The first layer of Monitor AI includes advanced algorithms for facial detection, motion, and lighting to analyze the student and examination environment. The next layer uses data from the computing device (keyboard activity, mouse movements, hardware changes, etc.) to identify patterns and anomalies associated with cheating. Finally, the student's interaction with the exam instrument itself is woven into the analysis, including question-by-question comparisons with other students who took the same exam.
>
> In all, Monitor AI analyzes dozens of factors, such as whether multiple faces appear within the video frame, or if the person who started the exam switches to a different person along the way. The data then flows into the "Review Priority" system to help instructors quickly evaluate the proctoring results.

## Respondus's Terms of Service

To use Respondus, students must agree to their terms of service[2] upon launching the software. However, students are not informed of this until their exam begins. If a student refuses to agree to these terms of service, then they would be unable to write their exam and would likely fail the course. Because students are not informed of this requirement prior to their registration in the course, it is unfair to require them to enter into a contractual agreement with a third party.

In addition, there are a number of problematic clauses in the terms of service. One particularly egregious clause specifically disclaims both Respondus's and [redacted] responsibility to secure my personal data:

[1] https://web.respondus.com/he/monitor/
[2] https://web.respondus.com/tou-monitor-student/

> By agreeing to these Terms, you agree to use Respondus Monitor at your own risk, and agree that Respondus shall not be liable if a security breach occurs, if the site malfunctions, or if information is misused or mismanaged in any way to your detriment or the detriment of a student or third party, whether by Respondus, your institution, or an unauthorized third party.

I am very concerned about the security of my personal data, and this clause makes me uncomfortable because it means that neither Respondus nor [redacted] have any incentives to maintain absolute control over my data.

In addition, by agreeing to the terms of service, I am agreeing that "Respondus reserves the right to change these Terms at any time, at its discretion, without advance notice to [me]." Once again, this clause is worrying because it means that I cannot have any confidence in Respondus to control my data. Since they can change these terms at any time, there is no reason for me to be confident that they will keep my data secure and private. If, for example, Respondus wanted to use my data in a way that I had not specifically consented to in the terms of service, they could simply modify their terms of service—even after they possess my data and we have otherwise terminated our relationship.

Also, the terms of service allow for Respondus to conduct research on my data at will.

> 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 (research institutions and/or biometric experts) under contract with Respondus to assist in such research.

I find this very problematic because now Respondus is specifically stating that they will share my data with third parties for the purpose of "research." Although they state that "no personally identifiable information for students is provided" to the researchers, a video containing my face is inherently personal information.

According to Respondus support documents[3], all videos are retained on their servers for a period of 5 years. During this time, my personal information is still subject to all of the concerns listed above. In fact, the Respondus terms of service[4] state that "Respondus does not guarantee removal of all traces of any information or data (including recordings) from the Respondus Monitor Services after deletion," therefore I can never be certain that my data will stop being retained by Respondus.

[3] https://support.respondus.com/support/index.php?/Knowledgebase/Article/View/180/26/how-long-is-video-kept-what-if-we-need-a-longer-period
[4] https://web.respondus.com/tou-monitor-student/

## Data Collected

In their advertising, Respondus states[5] that they monitor "keyboard activity, mouse movements, [and] hardware changes [] to identify patterns and anomalies associated with cheating," and in their privacy policy[6] they state that they may monitor and record "keyboard and screen activity." This is also very alarming to me because the Alberta *Information And Privacy Commissioner* ruled that keystroke monitoring is personal information[7] because it can show one's "style or manner of doing [work]". This invalidates [redacted] advice about how to maintain my privacy while using Respondus because there is no way to avoid transmitting my keystrokes to Respondus if I choose to take the course. Even more concerning is that Respondus does not consider the records of one's keystrokes to be personal information, therefore I have little confidence that they will take efforts to protect it.

In [redacted] initial response to my concerns, he stated that "if [I am] concerned about [my] privacy over the webcam, it is recommended that [I] situate [my]self in an unoccupied space and remove [] any personal property," however, this does not entirely alleviate my concerns. Although a minor concern of mine is the recording of my surroundings, my primary concern is that *I* am being recorded. I do not want for my image to be recorded and retained, and I cannot remove myself from the video stream if I am required to use Respondus.

## Data Storage

Another concern of mine is that Respondus is an American company and all of their data is hosted on US servers. This is a serious concern of mine due to the American government's propensity for surveillance without judicial oversight. Although the biggest revelation of the extent of the surveillance came from Edward Snowden back in 2013, the same practices continue today. In fact, the European Union just recently banned corporate data transfers[8] to the US unless a company has entered into a special agreement. Although this ruling only affects the EU, it shows that many American policies are fundamentally incompatible with the protection of individual privacy.

In [redacted] email—forwarded to me via [redacted]—he stated that "only the instructors of the Blackboard course can access the Respondus recordings," however this is demonstrably false. Respondus staff and any third-party researchers that they authorise

[5] https://web.respondus.com/he/monitor/
[6] https://web.respondus.com/privacy/privacy-additional-monitor/
[7] https://www.oipc.ab.ca/media/124840/F2005-003Order.pdf
[8] https://www.bbc.com/news/technology-53418898

have the ability to access my recordings, in addition to the US government. In addition, Respondus states[9] that institutional administrators [redacted] Staff) also have the ability to access the recordings. Now, [redacted] may have policies in place that only allow the direct instructors to access recordings, however these policies cannot prevent any third parties such as those listed above from accessing my data.

## Facial Recognition Bias

One other concerning aspect of the Respondus software is its use of facial recognition. This is specifically concerning because of the well-known biases of facial recognition software. In a recent paper[10] published by the US Federal government, researchers tested over 189 different algorithms and found that many of them exhibit demographic-dependant biases:

> False positive rates are highest in West and East African and East Asian people, and lowest in Eastern European individuals. This effect is generally large, with a factor of 100 more false positives between countries. [... Some of] the highest false positives are in American Indians, with elevated rates in African American and Asian populations; the relative ordering depends on sex and varies with algorithm. We found false positives to be higher in women than men, and this is consistent across algorithms and datasets. This effect is smaller than that due to race. We found elevated false positives in the elderly and in children; the effects were larger in the oldest and youngest, and smallest in middle-aged adults.

Now, none of this affects me directly, however it is concerning nevertheless. Many students who attend [redacted] fit into one of the minorities listed above, and this could have a detrimental effect on them. Although the above study shows an example where people are confused for other people, a similar scenario occurred with Google[11] where people were not even recognised as humans. Respondus states that their software "flags" videos where a human is not recognised in the frame so that they may be manually reviewed. If Respondus's algorithm has the same flaws as many others. this could lead to racial minorities being subjected to increased scrutiny during their exams.

## Advance Notice

Another issue with the requirement to use Respondus software is that it has completely different computer requirements than were disclosed prior to registration. The [redacted]

[9] https://support.respondus.com/support/index.php?/Knowledgebase/Article/View/179/26/who-can-view-videos-of-students-taking-exams
[10] https://doi.org/10.6028/NIST.IR.8280#page=5
[11] https://www.cbc.ca/news/Google-apologizes-after-app-mistakenly-labels-black-people-gorillas-1.3135754

[redacted][12] states that "Blackboard works on Chromebooks, Android and iOS devices," however Respondus only functions on a Windows or macOS device with administrator access[13]. The [redacted] site above states that "if you are completing an online test [] we recommend doing so on Windows or Mac computer," however that is only a "recommendation" while the operating systems are listed as a "requirement." In addition, Respondus requires a webcam. However, the [redacted] requirements site does not state that a webcam is a requirement; rather, it states it near the bottom as a recommendation if a student chooses to participate in a video conference. It is not fair that [redacted] expects students to have software and hardware that is not listed in the official "Computer Requirements;" however, Respondus will not function with some of the configurations that are listed as acceptable.

In addition, the first time that any of the students could be aware of the requirement to use Respondus was effectively the first day of class. This is because the first location where instructors mention the mandate to use Respondus is in their course outlines. However, the majority of instructors do not open their Blackboard site—which is where the course outlines are primarily hosted—until the first day of classes, therefore students never had a chance to know about the Respondus requirement until the term began.

## Legality of Data Collection

The *Freedom of Information and Protection of Privacy Act*[14] governs the use and collection of personal information by public bodies in Alberta. Pursuant to *FOIP* §69, the *Information and Privacy Commissioner* has the authority to begin an investigation into a public body's incorrect collection of personal information. Upon the termination of an investigation, he may issue an order that is binding upon the affected parties. One order that is very significant to the matter at hand—OIPC Order F2005-003[15]—is quoted extensively below. [emphasis mine]

> Summary: [...] The Commissioner found that the [the public body] did not have the authority under section 33 of the Act to collect the Applicant's personal information that it collected through keystroke logging. Noting that less-intrusive means were available for collecting information needed for managing, he held that the keystroke logging program collected information about the Applicant's activities during working time that was not necessary to manage him in the circumstances. [...]

[12] [redacted]
[13] https://support.respondus.com/support/index.php?/Knowledgebase/Article/View/172/0/what-are-the-system-requirements-for-respondus-monitor
[14] https://www.qp.alberta.ca/documents/Acts/F25.pdf#page=40
[15] https://www.oipc.ab.ca/media/124840/F2005-003Order.pdf

Discussion of Issue: The information that a person types into a computer in the course of performing their work activities may or may not be personal information. [...] In this case I [the Commissioner] am of the view that if most or even all of the information that was collected was the Applicant's work-related activity, all of it had a personal component in this case, because it was to be used to determine how much work he did, or his style or manner of doing it, or his own choices as to how to prioritize it. Thus in my view the collected information included personal information of the Applicant. [...] The Public Body itself provided evidence that its managers intended to review this information a couple of weeks after installation to determine exactly what the Applicant was doing on his computer. [...]

It is notable that the Director did not testify that she raised any concern with the Applicant at this interview that he was insufficiently productive or, (more specifically), that he was not completing a sufficient number of "trouble tickets" – the primary activity to which he had been assigned. The Applicant's testimony supported that there was no discussion or warning about under-productivity. [...]

In my view, the Public Body has failed to demonstrate its authority to collect personal information under section 33(c) in this case. The keystroke information that was collected in this case was not information necessary for management of the employee, and thus section 33(c) did not provide authority for the Public Body to collect it. [...] In my view it was not necessary for the Public Body's managers to know every single thing the Applicant did on his computer in order to know if he was being productive or prioritizing his work according to their instructions. They did not need all this information, or information of this particular type, in order to manage him effectively. [...]

In my view, information collected by keystroke logging software becomes "necessary" within the meaning of section 33(c) of the Act only when there is no less intrusive way of collecting sufficient information to address a particular management issue. [...]

If an employer had reason to believe an employee was using office equipment to surf the net on office time, information collected by keystroke logging software could become "necessary." However, this would be only after the employer had developed and conveyed to the employees a written "accepted use policy" relative to their computers. [...]

[This collection of information] would be considered "necessary" within the meaning of section 33(c) only when the information needed for managing could not be obtained by other means. [...]

> Order: I conclude that the Public Body collected the Applicant's personal information in contravention of section 33 of the Act.

Although it may not appear that this decision is directly applicable to my current situation, I believe that the majority of it applies.

First, the jurisdiction of the *FOIP Act* applies to the college under §1(d)iii. Since [redacted] is an organisation under the *Post-secondary Learning Act*, it is considered to be a public body, thus all of the same laws cited in the Order above apply to the college.

Second, both [redacted] and the public body above are using keystroke monitoring software. While much has changed in the world of technology since 2005, the reasons listed above for why this is personal information still apply. In fact, the situation at [redacted] is even more egregious because the College is also collecting the video and audio from students, and it is using a third party to collect and retain this information.

Third, the Applicant above had never been issued any warnings about his performance—formal or otherwise. This also applies to me: I have never received any warnings or punishments related to Academic Dishonesty at [redacted] or any other educational institution.

I believe that the above scenario is sufficiently similar to our current situation to deduce that [redacted] has no authority under *FOIP* §33(c) to collect this information, thus it cannot require students to install and use the Respondus software without violating provincial law.

## Conclusion

I realise that the current pandemic has made traditional methods of teaching impossible; however, this does not justify the use of Respondus as a substitute. The *FOIP Act* only allows information collection consent when there is an imminent danger to health, which is not applicable since the provincial *Public Health Emergency* has been lapsed since June[16]. The *Alberta Office Of The Information And Privacy Commissioner* has released a statement[17] specifically stating that all information collection laws still apply and consent is still required.

[16] https://globalnews.ca/news/7067163/alberta-health-covid-19-june-15-coronavirus/
[17] https://www.oipc.ab.ca/resources/privacy-in-a-pandemic-advisory.aspx

I am not comfortable using the Respondus software, and I will refuse to use it, even if required to do so by my instructors. I truly want to write my exams and achieve excellence in my studies; however, the current policies are nothing but a hinderance. Please take my concerns into consideration so that we can find a solution that is satisfactory to all.

Thank you for your time and consideration.

Sincerely,