Dear Dr. Hussein, Dr. deMontigny, and software systems faculty members,

Thank you for the detailed response to our last email. However, there are still many unmet concerns with Proctortrack and responses that we respectfully disagree with. We believe from a privacy and ethics perspective this is an important issue. Having learned about ethics and privacy in our courses starting in ENGG 123, continuing in ENSE 374 and ENSE 475, ENSE 400 as well as other courses, this is ignoring many of the main points we learned. In addition to these courses, we can understand that this is an ethical issue outside of our engineering knowledge and experience. We appreciate the time taken to read and respond to our last email. This email is very long and is the work of lots of research and consideration during our busy academic schedule. We appreciate the time it will take to read, understand and respond to this email and thank you for your time and effort. We request that the software faculty take the time to read this and support us in not implementing this software in our courses. There are headings in the email that are used to indicate what we are responding to from your response. The longest section of this is the FAQ which was enlightening in some aspects and deepened our problems in many others. Thanks in advance for your time and effort.

We are again asking the faculty to refuse to use e-proctoring solutions in all of their courses and have discussions with students regarding adequate alternatives. We ask that you join the over 2,200 students who have signed the petition calling for the removal of Proctortrack from the University. Please reevaluate the ethics involved in this decision and support the students who are not being heard by the University.

FAQ

We have thoroughly read the remote proctoring FAQ for students at https://www.uregina.ca/term-updates/students/remote-proctoring.html. This was used throughout the last email as part of our concerns with Proctortrack. Below we discuss most of the FAQ sections that are cause for concern and raise questions about the ethical nature of the software, use of personal information and general privacy concerns. If a FAQ section is not specifically addressed, it is either self-explanatory or covered with our concerns in other sections and would be redundant and add to the length of the email.

In the FAQ section "*How does Proctortrack work"*, steps 2 through 5 are areas for concern. The identification and verification of a student and their ID through the comparison of facial features stored on a server is aggressive and a great source of data in the event of a leak. As well, Proctortrack only allowing software allowed by the instructor is great in theory, but it has serious drawbacks. Using a work laptop, this might not be possible or it may cause issues. Additionally, if Microsoft Word is the software that is allowed by the instructor, alternatives such as the FOSS LibreOffice Writer or the use of Notepad, Notepad++, Pages or other text software would not be allowed. This is a technical issue, but an issue none the less as it pushed students potentially towards paid software that would add to the financial burden of the University. In Step 4, recording the webcam, computer screen and software running is particularly invasive and provides personally identifiable information.

In the "*Is the use of Proctortrack mandatory?"* section, Proctortrack is mandatory when a course instructor requires it. It should be noted that instructors are unable to force students to have cameras on in Zoom which is considered to be an invasion of privacy, but they are able to force remote proctoring on students which stores your video, screen and software and device information. This seems counter-intuitive as this is even more invasive and prone to privacy issues. Although it is not mandatory, it should not be able to be used without alternatives such as Zoom or other options available. Currently, the only

options are to use Proctortrack or drop the courses that are using it, these are not acceptable options in any way.

In the "*Will I have to pay to use Proctortrack?"* section, it states that there is no cost. There is a cost to the University however correct? How is this being recouped? Has tuition been raised and the price included, but not explicitly stated or is there truly no cost to students? We want to believe this, but also want to confirm our understanding on the issue.

In the "*What personal information is collected by Proctortrack?"* section, this is identifying information and the recording of video, audio and your computer screen and software running is extremely invasive. Having Zoom access your camera is considered invasive and some are uncomfortable talking on mic with Zoom. With Proctortrack, your screen, mic and video, as well as software running on your device, is then recorded and stored for up to a year. If more students were aware of this we believe there would be a greater outcry.

In the "*How does Proctortrack verify identity and track progress?"* section, we understand that later on you addressed concerns of identity verification. We also understand that students can complete onboarding earlier in the semester to ensure that things are working smoothly. This is not an acceptable solution as at this point they already have your data and are able to store it for 365 days as per Proctortrack's FAQ. When a student has trouble, currently there are limited options other than to drop the course which is an unfortunate alternative. We have read about the onboarding process and the purpose of completing it earlier is to reduce errors and the severity of issues, if and when they arise. We also understand that hopefully issues regarding facial features would be reduced, but this does not entirely eliminate them.

We have a question about the section "*What information does a student have to provide to use Proctortrack?"* where "Students are strongly encouraged to use their U of R Student Identification Card". Why are students "strongly encouraged" to use their U of R Student Identification to use Proctortrack? If the university would say "We encourage students to use their student ID for ease of use" this would be more transparent and provide a rationale. Currently, the statement leaves us confused and concerned. It would seem that if the University had trust in the system and that Proctortrack was secure, this would be unnecessary and any identification card, such as a government-issued photo ID, could be used without concern.

The "*Does Proctortrack really scan my knuckles?"* section states that the University of Regina is not employing knuckle scans. We appreciate this decision by the university and believe it is the right one. Unfortunately, the software still has the capabilities to scan and store knuckle information if incorrectly configured or taken advantage of by a third party. Although the intent is to not scan or store this, the software maintains its capabilities to do so. The safest action would be a software that does not have the capabilities such as a hypothetical Proctortrack light which is less invasive and has toned down capabilities.

With the "*Where can I find more information about Proctortrack and how the University will use Proctortrack?"* and "*What steps is Proctortrack taking to protect students' privacy?"* sections, we have read the Proctortrack's privacy policy and researched more about it as we will discuss below.

In the "*What steps is Proctortrack taking to protect students' privacy?"* there is a link to the privacy policy and the terms of service for Proctortrack. If you read the privacy policy, at a quick glance it was

last updated on September 15th, 2020. Consent is given to the privacy policy when you launch the server, register or login, request customer support or more information or have provided biometric data. Since we are forced to use this software, we are forced to consent to the terms. This consent is not given willingly and is therefore under duress and not valid. Proctortrack can collect your name, photograph, email, test submissions, screen-captures, audio and video recording, room scans, biometric data and hardware and software details. This is personal information that a single program should not have access to. The room scan is vague and provides the potential for the scanning of documents or people in the area that should not be recorded. Verificient states that it does not share or sell any information to third parties. But, then goes on to state, "In the case of any merger, sale, acquisition, bankruptcy, liquidation, or other transfer of assets involving the company, any of your personal information which remains on the company's servers at that time, may be transferred to and / or managed by the acquiring company or entity". This means that this privacy guarantee is not guaranteed past the company's life. While generally reasonable, with so much data from students across Canada and the United States as well as internationally, this makes them a very valuable source of data. Under "Changes to this policy" they reserve, "the right to change this Policy from time to time by posting an updated policy to this site and the "last updated date" at the top of this page will be updated.". This allows the policy to be changed without the knowledge of the university or the students using it through the university. Any protections of data and personal information could be removed. This agreement is made on the trust that the privacy policy will remain constant and this is not a guarantee. As well, in the "*The Choices You Have With Your Information*" section of the privacy policy, "it is not always possible to completely remove or modify information in our databases". This statement is concerning as the control that one usually has over one's data is not being upheld by Verificient. This is an extremely unethical system and cause for legal concern. In the Terms and Services, under section 6, "*Limitations of Liability*", the claims in i, ii, iv, vi, and vii are extremely problematic. Verificient takes no responsibility for "direct, indirect, incidental, special, punitive, exemplary, or consequential damages" resulting from using their services, "errors, mistakes, or inaccuracies", "unauthorized access to or use of, corruption of, interference with, or alteration of our secured servers and/or any and all personal information and/or financial information stored therein", "any bugs, viruses, trojan horses, or the like, which may be transmitted to or through the Verificient Services by any third party", and "any errors or omissions in any Content or for any loss or damage of any kind incurred as a result of your use of or reliance on any Content posted, emailed, transmitted, or otherwise made available via the Verificient Services". The statements surrounding points i, ii and vii, are concerning for their lack of responsibility in errors and issues with remote proctoring and any consequences that arise from accidental reports of academic misconduct. Taking no responsibility for errors surrounding their main service is to protect them legally, but they should be held responsible if something were to occur. Point iv with respect to privacy is extremely problematic. The statement that Verificient is not liable for "any unauthorized access to or use of, corruption of, interference with, or alteration of our secured servers and/or any and all personal information and/or financial information stored therein" should not be acceptable. Any unauthorized access should be their problem and the University should hold them accountable. How the University agrees to these terms and accepts a company who will not take responsibility or expects us, as students or software engineers, to agree to this is ridiculous. Again, the terms of service are subject to change and Verificient is not responsible for notifying anyone of these changes. Even if the terms of service or privacy policy do change, Verificient have our data and we are unable to withdraw our consent or refuse to use Proctortrack. The terms of service and privacy policy could be changed and written up by the University and entered into contract with Verificient, but based on the links to Verificient's public privacy policy and terms of service we assume that this is not the case. In the event that this is the case and the University has negotiated separate terms or a separate privacy policy, this should be linked to and made public instead.

https://www.proctortrack.com/privacy-policy/
https://www.verificient.com/terms-of-service/

"*What steps is the University of Regina taking to protect students' privacy when using Proctortrack?"* in the FAQ claims that the "The University of Regina is committed to protecting students' personal information and has reviewed Proctortrack's security and data management practices with this commitment in mind. The data protection practices established by Proctortrack meet or exceed industry standards to prevent unauthorized access to the records, taking into account the confidential nature of the records to be protected.". This is an encouraging claim and a good start. The link to the Freedom of Information and Protection of Privacy contains many resources. In the LOCAL AUTHORITY FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY Act and Regulations document, under "Confidentiality provisions in other enactments" *section 8.2* it would appear that "(b) provisions setting out the obligations of the information management service provider respecting the security and safeguarding of personal information; and (c) provisions for the destruction of the personal information, if applicable". These requirements are not met by Proctortrack and the University in its disclosure to students. In your reply under the heading "*Privacy*" we value the admission that ensuring the privacy of students to the greatest extent possible is important. We understand that personal information collected is stored on Proctortrack's Canadian servers which is important. This potentially avoids the overbearing Patriot Act that allows the United States Government access to any data, anywhere and anytime. However, is there a guarantee in place to ensure that no data flows to a Proctortrack node in the United States on its way to Canadian Servers? This is a common problem and the storage being in Canada does not necessarily protect students from the Patriot Act. We would be interested in the privacy obligations and how Proctortrack meets them. This would also meet the *section 8.2.b* requirement of outlining the obligation to disclose the provisions. Is the screen capture, video capture and audio capture also encrypted? Reading your email we are unsure if this is included in personal information and encrypted and would appreciate clarification. As well, the encryption suite that they are using would be important to know, as their server report shows they allow weak encryption methods. We believe informing instructional staff of how to handle any data collected by Protortrack would seem to be only following the mandate set out in the Freedom of Information and Privacy Act. The Freedom of Information and Protections of Privacy Act in section 11 outlines the requirements for consent for use or disclosure of personal information. In section 11.1.b, the collection of personal information the individual must be "informed", "given voluntarily" and "not obtained through misrepresentation, fraud or coercion". Although the university has provided some details on how personal information is collected and used, the storage is not completely transparent and students who are protesting the use of Proctortrack would not be voluntarily providing their consent. The university is forcing students to provide consent and providing the only alternative of dropping out (which is now only possible without a refund). This seems to go against the Freedom of Information and Protections of Privacy Act. The University also misled and misrepresented the capabilities of the software publicly in the interview with CBC, linked previously, which also violates section 11.1.b.

The Privacy Breach Protocol in Appendix II of the Freedom of Information and Privacy Act claims that the breach will be contained. This seems difficult with an external company in control of the servers and data. The rest of the document and procedures outlined in it is good though. The concern with a breach though, is that many companies have covered up massive data breaches to avoid consequences and bad press. Uber most recently, Cambridge Analytica and other high profile companies. This is a concerning trend with software companies and hard to guarantee that it would not occur in the event of a breach. We assume that there are strict regulations in place and consequences for a data breach and would be interested in more transparency surrounding this. In the case of a breach, the data is already

exposed and the damage is done. Is there monetary reparation for students in place? Although this would still be unacceptable.

In "*How is the data stored by Proctortrack and for how long?"* section of the FAQ, 365 days seems overly long as the semester is roughly only a third of that and the storage of identity verification is extremely personal. This also would appear to be against the consent section 11.3 where consent may be given that is effective for a limited period of time. If consent were to be given for a limited period of time, the data is still stored for the 365 days.

"*What steps can I take to protect my privacy when using Proctortrack?"* again indicates the use of a student ID is preferable to a government-issued ID and that when using a government-issued ID personal information should be covered up. This section contains a lot of good advice to protect privacy, but the fact that your privacy is so compromised by the software is concerning. This is invasive software that records you in your home, your family or partner, and audio in the environment. This section seems to indicate concerns that the University has with long term use and storage of data. Although this is good practice, it is cause for the ethics and privacy policies in place to be questioned. These suggestions appear to show that the University is also concerned and if this is the case and they are misrepresenting the risks which seems possible, this would be in violation of section 8.2.b and 11.1.b of the Freedom of Information and Protections of Privacy Act.

The "*Is Proctortrack access to my computer terminated after my exam?"* and "*What information on my computer can Proctortrack access?"* are vague in their descriptions. If Proctortrack is running, in theory it does not collect data, but it maintains the capability to collect and transmit data. In addition to this, session data is also vague as it is able to access any software running on your computer and is not clear about the consequences of opening personal files. These capabilities can be leveraged by third parties and used to collect personal information.

Sections "*I am worried that certain behaviours may result in a finding of academic misconduct. For example, what if I tend to look up when I'm thinking, or fidget when I'm stressed?"* and "*Does Proctortrack determine academic misconduct?"* are hopeful for the proper use of the software, but the privacy concerns remain, even if wrongful convictions of academic misconduct are unlikely. In the event of a wrongful conviction of academic misconduct, Proctortrack does not take any responsibility for taking part in flagging 'areas of concern'.

The "*What if I don't have access to a quiet space or the right type of computer system to do my Proctortrack Student Onboarding and/or take my exam?"* section identifies the Library having eight quiet spaces available. In your email you state under the section "*How Proctortrack will be used for timed exams*" that, "[in] just over 100 courses ...it is being used", this seems like eight spaces would not be adequate even for a single course. Our courses have about twenty students in them, not all would opt to write at the University, but the available space is limited and this is unacceptable. As well, the option to write at the University does not protect our privacy from Proctortrack.

In the "What should I do if I do not have adequate technology (ie webcam, microphone or appropriate internet connection)?" section, the computer requirements are similar to what is required for online learning. However, this does not mean that this is acceptable for Proctortrack. We are skeptical about the IT Support Centre's ability to upgrade someone's internet connection if the area does not provide it or the person does not have the ability to pay for the upgraded service.

In general, we have thoroughly read the FAQ that the University provided, both prior to our first email and after your response. As you have read, there are various valid concerns that the University has yet to address. We would hope that these concerns, particularly those with the privacy policy of Proctortrack and The Freedom of Information and Protections of Privacy Act sections would impress upon you the problems with the use of the software.

Why Proctortrack is being used at the University of Regina

The argument that Proctortrack is being chosen at other universities is not acceptable. To use an engineering analogy, if all the companies are using a low grade material that is at risk for failure, this does not make this material safe or ethical to use. Simply because it is used by others does not make a product ethical or appropriate. We believe that any argument centred around "But other universities use it too" is dismissive and has a weak base.

We respect that teaching staff in a number of faculties may have requested the implementation of remote proctoring software. Again, this is unacceptable as these are teaching staff, and generally are not software or privacy experts. Students may also have expressed their desires for a way to ensure the academic integrity of their degrees. We agree that stopping cheating is important. We also agree that when people cheat it discredits your diploma and degree and makes it harder to get a job and the degree itself worth less. It is in our best interest to protect academic integrity and the integrity of this institution. However, in our courses last semester, we had the same situation and no Proctortrack or remote proctoring software. We had our cameras on for human proctors to supervise us and stop cheating and stop students from taking exams in groups. This is a viable alternative to remote proctoring software, especially in smaller class sizes that are present in upper level courses, and we request that the Faculty of Engineering encourage this solution.

Consultation

We understand that consultation has taken place in some aspects. However, as per our last email, the concern is that the consultation with students did not take place in high concentration and student participation. URSU represents students, but the executive council consists of a MAP student, an economics major and a psychology major. The executive council members are not experts in technology, nor are they experts in privacy and may not realize the invasion of privacy that Proctortrack is or the importance of this. The students who asked questions at the town hall may have had a more technical background though. The town hall held with faculty and staff is not a consultation with students. We believe that not enough consultation was done with students during this process and we would be interested in knowing how many students, out of the approximately 16,500 students the University has, attended the town hall and were consulted. As well, we admit that these town halls may not be overly well attended and would like to consider what attendance was like at other town halls for different issues in the past. As students, we have a right to be informed about University policies and we appreciate the transparency in your response, it has provided insight into information that was not available before.

We understand the work that went into the decision and how hard it would be to find a software that is able to perform proctoring remotely while respecting privacy. There is a lot of oversight and work involved in such committees. We understand that this may have been the best solution available out of

the options considered. Although it may have been the best implementation considered, we do not believe that it is an acceptable solution regarding the privacy policy and the privacy concerns surrounding it and other implementations of remote proctoring software.

We respect that Proctortrack has been tested beforehand, however, already there are issues coming up with Proctortrack implementations. Proctortrack requiring Microsoft Word, as mentioned before, and closing down LibreOffice Writer, a viable and accepted alternative. Questions not having values assigned is another problem as well. We understand that these are technical issues and potentially resolvable, but the existence of these issues is a source of extreme stress. The ability for Proctortrack to not work and to have technical issues caused by the software itself or of the teaching instructors' setup of it is complicated, but should be a source for investigation.

When Proctortrack will be used for timed exams

The University has not made remote proctoring mandatory for all exams in the Fall 2020 term. We agree with and support this decision and would strongly oppose mandatory use of remote proctoring in its current form in any future semester. We disagree with the professors that choose to use it for timed final exams and mid-term exams and make the use of Proctortrack mandatory in these situations. Forcing students to use a software, even when most students in a course disagree with it, is unacceptable. If exams would require full consent of the class to use Zoom with the cameras on, why is the full consent of the class not required for Proctortrack? However, this is exactly the case in one of our classes and currently is not resolved. This is a trend that we would like to see ended. When a class is collectively opposed to Proctortrack, this software should not be implemented. We understand that sometimes alternatives are difficult to undertake and ensure they appropriately assess students. In some cases, we believe this could be from professors continuing to use old exams and not wanting to update content to a form that would work with suggested alternatives. In other cases, there may truly be no alternatives, but this should be proven and verified to the students in an understandable way. We call on the Faculty to not support the use of Proctortrack and to encourage the use of alternatives instead. In the event that an alternative cannot be found, the Faculty should verify this as part of transparency as we cannot think of many exams that would not be doable with a Zoom camera on or a video recording sent to the professor.

How Proctortrack will be used for timed exams

We understand how Proctortrack will be used to verify a student's identity by matching the students' face to their ID. We disagree with the comparison to the requirement for in person exams. While students do have to verify their identity with their ID, the ID is not stored, their face and biometrics are not stored. It is a single person, your professor or teaching assistant, not a server that stores this data for a year and can be compromised at any point. Also, any comparison to exams taken in the gymnasiums would not hold up either. The cameras in the gym are not recording your screen, audio, running software, keylogs and collecting your private personal information from your computer. The cameras are controlled by the University and the University is responsible for the proper storage of footage. As well, many upper level exams are not taken in the gymnasium and would not be subject to this record-

ing regardless. Proctortrack is more invasive than the gymnasium exams or proctoring using cameras on Zoom.

We appreciate the explanation of what Proctortrack does in regards to flagging potential content. A brief look at Proctortrack's FAQ states that, "Proctortrack's role at universities is to highlight abnormal behavior and then present its findings to instructors"[1]. This is also stated in the CBC article previously attached, and on Rutgers, and Ohio University pages on Proctortrack [2,3,4]. The University's FAQ on Proctortrack under, "How does Proctortrack work?" does not specifically state this. We would like clarification, if this is misleading, whether intentionally or accidentally, or an actual implementation difference in what CBC, Rutgers and Ohio University state. We fail to see how Proctortrack is less invasive than real-time monitoring in Zoom. Although it might not be immediate feedback to the professor, the feedback and flagged content would be available after the exam is completed. With Zoom, it is your professor or TA viewing you and ensuring academic integrity. With Proctortrack, it is stored in a server and will be stored there for 180 to 365 days, in which time a breach might occur and that recording would be all the more invasive.

[1] https://verificient.freshdesk.com/support/solutions/articles/1000065467-how-does-proctortrack-catch-cheating-
[2] https://www.cbc.ca/news/canada/saskatchewan/university-regina-students-proctortrack-privacy-concerns-1.5734005
[3] https://canvas.rutgers.edu/external-apps/proctortrack/
[4] https://www.ohio.edu/oit/services/testing/online-proctoring

Privacy

We admire the commitment to privacy for all students even if this affects a relatively low number compared to the University population. As described above in the FAQ section about "*What steps is the University of Regina taking to protect students' privacy when using Proctortrack?"* there are remaining potential issues. We would be interested to know of the encryption and database security used. The database report attached in the last email is cause for investigation. And, security tends to be a commitment and a company lifestyle as we have learned in our software engineering courses. We find it hard to believe that Verificient would have tight and up-to-date database security if their main server is lacking. This has been discussed more thoroughly above and if you have limited time and missed it on first read through, we implore you to read the concerns on that section.

Identity Verification

The encouragement to participate in onboarding early, while helpful, is unacceptable due to the above mentioned privacy concerns which make it impossible to, in good conscience, ethically use this software. It is possible and we have learned a fairly quick process to obtain a student photo ID card about four of five days. We respect this suggestion and appreciate it. The concerns surrounding the encouragement of using a student ID instead of a government-issued one are outlined above in the FAQ section.

Hardware and Internet Requirements
The hardware components are relatively low admittedly and mostly required for online learning. We believe that the webcam will be the most problematic part. Webcam prices have been inflated by the increased demand for them and many people with desktops will not have one. Inconsistent shipping with Canada Post and FedEx having long wait times due to the pandemic also makes obtaining one hard as we move closer to midterm exams that might need them. The IT Support Centre might be able to help, but depending on the demand they could be overwhelmed. Proctortrack reportedly does not work on Linux, or a VM running Windows within Linux. This is an unacceptable requirement that again pushes students away from FOSS and towards paid software. Many software engineering and computer science students use Linux as their main operating system as well as other students in the University. The eight quiet spaces to write in the University to potentially fix this does not work for those who were under the impression that they could write exams and participate in courses completely remotely. If a student is in their home province or in a different country, these options provided with the Library spaces and the IT support will not be helpful. We are optimistic that every student might meet the requirements, but the problems would be a source of stress.

In closing, we have thoroughly researched Proctortrack, reading their privacy policy, terms of service, FAQ, the University's FAQ, The Freedom of Information and Protections of Privacy Act and using other sources for both this email and the previous one. We thank you for responding to our concerns and hope that our more detailed list will bring some clarity. We understand that this email is long, but we wanted to be thorough and ensure that the information provided was accurate and voiced our specific concerns with University policies and messaging surrounding the software. We remain skeptical of the ethics surrounding such a software and concerned about the invasion of privacy that it is. We are concerned with the example this sets for authoritarian surveillance and overbearing, privacy-invading software in the future, implemented by schools, workplaces or the government. To be quiet and complicit in this is something we cannot accept and stand for. We again call on you to understand and respect students and stand with us for our privacy. There are many important aspects of our courses that relate to this issue and the professors of this faculty have impressed upon us the need to act ethically and to protect the privacy of users. Proctortrack does not appear to be ethical or privacy protecting software. Ethics is a pillar of engineering and we hope that as a Faculty you can demonstrate that to us, as future engineers.

Thank you,

Avery Cameron (4th year Software System Engineering)

Noah Rowbotham (4th year Software System Engineering)

P.S
As a side note, Verificient also has monitoring "solutions" for remote employees under RemoteDesk. They claim that it is an employer's right to monitor employees aggressively. Please consider what

would happen if the University or any other company was to have you install this software and the outcry this would cause. How would you feel having your privacy violated, important and confidential documents and research potentially leaked? Our complaints and concerns stem not only from current use in the University, but the changes it would cause in the business world if we were to be complacent and not voice concern for Proctortrack and this invasion of privacy.