Online proctoring: Privacy and risk management considerations for schools

23 avril 2021

The shutdown of universities and colleges in the early days of COVID-19 triggered a rapid shift to online learning and online testing. Enter online proctoring, which has attracted scrutiny from privacy advocates at many post-secondary institutions.

Universities and colleges (together, "schools") use online proctoring tools to verify who is taking a test and to identify cheating. Online proctoring tools facilitate the proctoring that has long occurred in exam halls and test centres, but connect test takers with their proctors over the internet. They work by collecting, using and often recording personal information about students, including student images and images of student homes, information about test taking activity, and biometric data such as fingerprints, facial images, voice recordings, or iris or retina scans.[1]

While schools made the transition to online learning quickly, many were unable to assess the privacy and risk implications of online proctoring before implementing it. Now that the pressures of this transition have subsided and schools have built an understanding of their new model of academic delivery, it is an opportune time to revisit the privacy impact and risks of online proctoring and make adjustments. This bulletin provides privacy and risk management guidance to schools that may help.

1. What is online proctoring?

Online proctoring involves the use of software to monitor students during the administration of remote exams and assessments.

Some online proctoring tools support "live proctoring." With live proctoring, students interact with a proctor over an online video connection. Proctors may ask students to identify themselves and scan their environment for items that appear to be unauthorized aides. Proctors may then monitor students via webcam, either with or without recording the exam.

Other tools support "automated proctoring," which relies on software to flag suspicious behavior and to prevent the use of other computer functions during an exam–for instance, shutting down access to the internet and email or disabling the use of copy and paste.[2] Targeted behaviors can include such things as looking away from the

computer for a prolonged period, reading aloud to oneself, or reaching to grab something out of frame.[3] Automated proctoring tools flag suspicious behaviors for human review, usually by a professor or teaching assistant.

2. Privacy considerations

Necessity and legitimate purposes

Under privacy laws, schools can collect personal information only as "necessary" for a "legitimate purpose."

When considering this threshold privacy question, schools should do more than rest on broad assertions about maintaining academic integrity. Although maintaining academic integrity is an unquestionably legitimate objective, the scope of the need for online proctoring relates closely to the risk of academic dishonesty. It may help, then, to develop a risk model that sets out, for any given assessment scenario:

- The risk of academic dishonesty (degree and form); and
- The impact of academic dishonesty.

Different populations of students and different forms of assessments are associated with different degrees of risk. Moreover, the risk of identity fraud (which serves as strong justification for online proctoring) may differ from the risk of other forms of dishonesty. Regarding risk impact, the impact of dishonesty may be tolerable for assessments worth a small proportion of an overall grade.

A strong risk analysis may reveal opportunities to minimize privacy impact. Questions to consider may include, for example:

- What assessment scenarios warrant the use of online proctoring?
- What features should be enabled or disabled for different assessment scenarios?
- How can the impact of asking for identification be minimized? Should students be required to show proof of identity? Will student cards suffice for this purpose?
- How long does video footage of students need to be retained in light of the applicable academic dishonesty policy?

Schools should strive to use online proctoring effectively and in a manner tailored to the risk of academic dishonesty. We are not suggesting that schools impinge on academic freedom, so much as provide clear and direct guidance to faculty to promote the consistent and sound use of online proctoring tools

Schools that take this approach will invite the sound exercise of academic discretion, and will deserve deference from privacy regulators in the event of challenge.

Staff training

Schools should consider how best to educate their staff on the appropriate and privacy-friendly use of the online proctoring tool. Such training might address:

- When and how to use online proctoring tools;

- How to accurately interpret flagged behaviors;
- How to minimize the need for video review;
- Confidentiality obligations associated with access privileges; and
- Where to provide feedback on accuracy concerns or report privacy or security problems.

Faculty and other staff who review flagged behaviors are in a unique position to assess the accuracy of the chosen tool and its settings. Schools should consider periodically gathering data about accuracy and making adjustments as necessary.

Vendor due diligence

When adopting any technical service for processing student personal information, schools should employ vendor due diligence – *i.e.*, a set of risk management activities that entails selecting a vendor, incorporating contractual terms (regarding data governance and security), and administering the vendor-school relationship. Due diligence for online proctoring tools is not unique, and invites such questions as:

- How does the vendor use data? Is any use of aggregate data appropriate?
- Does the vendor disclose the personal information to third parties? Are there appropriate assurances regarding subcontractors?
- Where will data reside? How will it be secured?
- Will the data be securely disposed of on request and at the end of the contract?

Transparency

Schools should give notice of collection as required by applicable privacy law, but should also strive for strong transparency. Communications with students should include information about how online proctoring works, with simple, plain language summaries and links to more detailed vendor information. Schools should consider providing students with guidance on where best to take an online test and on removing personal effects from their test taking environments.

Opting out

Schools might also consider whether students should be allowed to opt out of using the online proctoring tool. This type of opt-out mechanism would need to be crafted in such a way as to not make it excessively easy to opt out, while still giving students a reasonable opportunity to opt out in specific circumstances. While not easy to design, such a mechanism would have many benefits from a privacy perspective.

3. Risk management considerations

Vetting online proctoring findings

Online proctoring that relies on automated software creates a risk of “false positives,” meaning instances in which a student’s mannerisms or movements are incorrectly interpreted as indicating cheating behaviour. For example, one commentator has written about a student who alleges that she was flagged for covering her eyes during an exam,

which she said was an involuntary movement triggered by her anxiety disorder.[4] Commentators have also expressed concern that neuro-divergent students may be unfairly "flagged for things like moving their eyes with increased frequency".[5]

This prospect of "false positives," and the possibility that they may disproportionately affect students with health concerns or disabilities, raise important considerations. Schools should ensure that a teacher or school administrator receives and manually reviews each flag produced by an online proctoring tool, so that any suspicious behaviour identified by the tool is closely vetted by a human being before it is relied on as potential evidence of wrongdoing. Consideration should also be given to keeping track of the accuracy of these flags.

Integrating online proctoring into existing academic discipline procedures

Schools are encouraged to ensure that, once a flag raised by online proctoring is appropriately vetted, it is handled within the school's existing framework for suspected academic dishonesty. This way, existing rules in respect of transparency, burden of proof, and procedural fairness will be applied and followed as appropriate.

Conclusion

Schools have implemented online proctoring with remarkable agility and under significant time pressures. Now, as the pandemic enters its second year, it may be prudent for them to think more carefully through the privacy and risk implications of this important shift.

[1] Mary Retta, "Exam Surveillance Tools Monitor, Record Students During Tests" (26 October 2020) *Teen Vogue* [Retta].

[2] "4 Popular Myths About Remotely Proctored Exams Debunked" (28 January 2020) *Proctor Track* .

[3] Drew Harwell, "Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance" (1 April 2020) Washington Post.

[4] See Retta, *supra* note 1.

[5] *Ibid*.

Par

Ira Parghi, Daniel J. Michaluk, Rebecca Flynn

Services

Litiges, Technologies de l'information, Cybersécurité, respect de la vie privée et protection des renseignements personnels, Éducation

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749