Information privacy and security in a virtual learning world

November 16, 2020

Introduction

In recent months, colleges, universities, school boards and independent schools (together, "schools") have found themselves scrambling to implement virtual education. While many schools have been deploying digital tools for years, this kind of widespread and complete shift to virtual education has been unprecedented. Although it has gone smoothly in many respects, there have been privacy and security challenges along the way. Virtual education technologies can capture, display, use, and record large volumes of personal information (PI), including students' images and voices, demographic information, and health data. Unfortunately, due to the COVID-19 pandemic, many schools have had to select and implement these technologies without being able to analyze their privacy impact.

Now that the urgent need to deploy new technologies has passed, it is a good time for schools to take a closer look at how their newly deployed technologies fare in a privacy impact analysis. Below, we offer a framework that encourages schools to consider each stage of a virtual education technology's handling of PI, from the time of collection through to disposal. The framework aims to help schools do the following:

- Ensure there is a defined process in place for making decisions about virtual education technologies – something that, in the context of public school boards, the Information & Privacy Commissioner of Ontario has encouraged;[1]
- Evaluate the potential privacy and security risks posed by each technology that is currently being used and that may be brought on in the future;
- Assess the extent to which any such risks may be mitigated by appropriate configuration of the technology (*i.e.* adjusting its "settings") or staff, student, or even parent education on the appropriate use of the technology or on privacy generally; and
- Articulate to students, families, and other stakeholders the process and principles that guide the selection of these technologies.

When applying the framework to a particular technology, schools should have regard to the technology's privacy policies and terms of use and should assess the risks in how a technology may be used or misused by students, teachers and even parents.

Schools are encouraged to tailor this framework as appropriate to their unique circumstances, and to draw on technological and legal expertise as required. We hope that it will serve as a helpful starting point as schools continue to navigate this new world.

Privacy and security assessments of virtual learning technologies: A suggested framework

The collection of PI

- What types of PI does the technology capture, and how?[2] Does it use "cookies"? What PI is recorded? What PI is merely revealed or broadcasted to others?
- Does the technology capture or collect more PI (*i.e.* more types of PI or a larger volume of PI) than the school needs? Are there lesson plans that would be appropriate in class that ought not to be conducted using the technology?
- If so, can this be addressed by configuring the technology differently? Or by educating staff or students on how to use the technology or on privacy practices generally?

The recording and retention of PI

- Is there any PI that the school needs the technology to record or otherwise capture, for legal or operational reasons? If so, which specific types and volume of PI? For how long does the school does the school need the recording to be retained?
- Does the technology record/capture any PI that the school does not need recorded/captured? Does it retain that PI for longer than the school requires?
- If so, does the technology enable a school administrator to remove recordings as needed? Or can recording and retention be addressed by configuring the technology differently? Or by educating staff or students on how to use the technology or on privacy practices generally?
- Does the technology enable others (students, parents) to record PI or access recordings of the PI?
- If so, does the technology enable a school administrator to remove recordings as needed? Or can this be managed by configuring the technology differently? Or by educating staff, students and parents how to use the technology or on privacy practices generally?

Access to PI

- Within the school, who has access to the various types of PI collected by the technology?
- Is this access appropriate, having regard to the role of each individual with access?
- If not, can this be addressed by configuring the technology differently? Or by educating staff on how to use the technology or on privacy practices generally?
- To what types of PI does the technology provider have access? For what purposes?
- Is this access appropriate?

- If not, to can this be addressed by configuring the technology differently? Or by other methods?

The use of PI

- How does the school use each type of PI that it collects via the technology?
- Are there any such uses that may not squarely map onto an educational purpose?
- What does the technology provider do with any PI to which it has access?[3]
- Is this use appropriate?
- If not, to what extent can this be addressed?

The display and disclosure of PI

- What types of PI does the technology display to staff and students while it is in use?
- Does the technology display more PI while in use than is required and appropriate?[4]
- If so, can this be addressed by configuring the technology differently? Or by educating staff or students on how to use the technology or on privacy practices generally?
- Does the school share any of the PI it collects through the technology with other entities? If so, what specific PI, with whom, and for what purpose?
    - Is this PI sharing appropriate? If not, to what extent can this be addressed?
- Does the technology provider share any of the PI to which it has access with other entities? If so, what specific PI, with whom, and for what purpose?
    - Is this PI sharing appropriate? If not, to what extent can this be addressed?

The safeguarding of PI

- What technological safeguards (*e.g.* encryption, two-factor authentication) does the technology use to protect the confidentiality of the PI that it captures and to limit unauthorized access to the technology?[5]
- Are those safeguards reasonable, having regard to the sensitivity of the PI, the amounts and types of PI, and the ways in which the PI is created, stored, and disseminated electronically?[6]
- Is the technology configured so as to adequately deploy those safeguards?
- What organizational or physical safeguards (*e.g.* privacy policies, staff education) does the school have in place to protect the PI and limit unauthorized access to the technology?
- Are those safeguards reasonable, having regard to the factors outlined above?
- Are the technology's practices with respect of PI, including these safeguards, articulated in its privacy policy? Would there be a benefit to sharing that policy with students and parents?
- Does the technology hold itself out as complying with any relevant privacy legislation? Would there be a benefit to communicating that information to students and parents?

The disposal of PI

- When PI collected by the technology is due for disposal, how is it disposed of?
- Is this manner of disposal sufficiently secure?

Conclusion

Schools are to be applauded for the agility and hard work they have demonstrated in deploying so much new technology so quickly. Thankfully, the privacy “bumps” that many have experienced in the rush to deploy were met with understanding from students, parents and regulators. As time goes on, this tolerance will become more limited. Whether they use the framework we have proposed or their own, we encourage schools to now conduct an assessment, identify under-managed risks and address them.

We thank our articling student Zoe Aranha for excellent research assistance with this article.

[1] Privacy Guide for Educators.

[2] Such collection may be active (*e.g.* a student enters in demographic data electronically) or passive (*e.g.* a classroom session is shared on screen). The latter can be trickier to identify.

[3] The Information & Privacy Commissioner of Ontario has warned that some digital educational technologies track students’ online activity; generate individual student learning profiles, based on students’ academic performance, which they then use to market products directly to students or parents; or sell student information to third parties (Protecting your students' privacy online).

[4] For example, there have been incidents in which remote learning technologies have sparked concern because they identify students in the virtual classroom via their legal names (also known as “dead names”), rather than their preferred names. This has resulted in some students’ transgender status being inadvertently disclosed to their classmates without their consent (see, *e.g.,* Inquirer: "Philadelphia school district transgender student coronavirus remote learning").

[5] For instance, there have been well-publicized “Zoombombing” incidents in which strangers gain unauthorized access into a virtual classroom environment (see, *e.g.*, "'Zoombies’ Take Over Online Classrooms").

[6] In assessing this, schools are encouraged to include consideration of particularly sensitive forms of PI that the technology may capture, such as clinical information about special needs students.

By

Ira Parghi, Daniel J. Michaluk

Expertise

Corporate Commercial, Cybersecurity, Privacy & Data Protection, Privacy & Security Breaches, Government & Public Sector

---

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

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 De La Gauchetière Street West
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