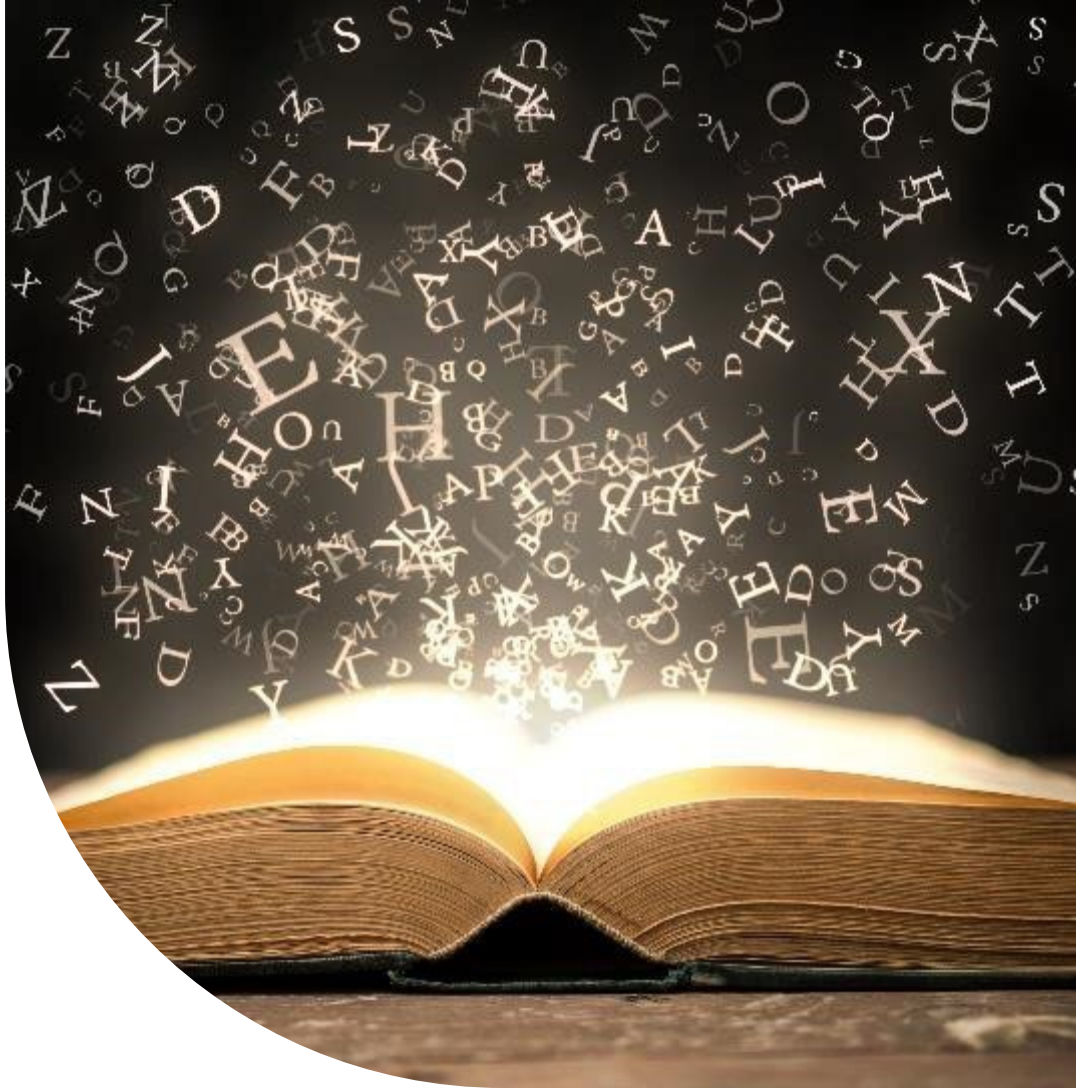
Striking a balance between innovation and privacy in educational settings



Presented By

Dan Michaluk

January 24, 2023

Borden Ladner Gervais

Welcome to January 2023!

How COVID Spurred Digital Innovation and Empathy

In the early pandemic, educators rallied to provide academic continuity in unprecedented ways. That spurred online teaching innovations, many of which are worth preserving and enhancing, a Stanford self-study says.

By Susan D'Agostino · Published October 20, 2022

Data analytics could transform student experiences, but higher education institutions need to gather and efficiently measure information

Higher Education Data Centers Move to a Cloud Operating Model

STUDENT ENGAGEMENT

As Student Engagement Falls, Colleges Wonder: 'Are We Part of the Problem?'

Learning from higher ed institutions that deliver support to students as the default, not the exception.

Ransomware Attacks Against Higher Ed Increase

Colleges and universities experienced a surge in ransomware attacks in 2021, and those attacks had significant operational and financial costs, according to a new report.

'We will not be doing that again.' Local schools report 'Zoom-bombings,' increase security measures

Welcome to January 2023!

The challenge

We are in a period of change and complexity, with opportunity and risk.

- Greater user demands
- Fragmentation of institutional networks
- More data, new uses for it
- Heavy burden on IT, IT security and privacy professionals at the institution

Higher education institutions are large and de-centralized, with limited funding

The needed response

- → *Innovation is a given, an imperative*
- → *We all must understand and address privacy risk as we go*
- → *Privacy and security is all of our responsibility*
- → *Individuals across the institution should build understanding and receive reasonable support*

Agenda

Begin your journey today

- Three privacy pillars
- Privacy for educators and educational administrators
  - Virtual work
  - Online academic delivery
  - Educational technology
  - Cloud computing
  - Privacy impact assessments
  - Managing privacy breaches

Three privacy pillars

Three privacy pillars

1

Act with a authority - Collect, use and disclose personal information fairly and as authorized

2

Minimize – don't collect, use or disclose without a real need... and minimize retention

3

Secure – reasonable administrative, technical and physical measures to protect

Privacy is about control over one's personal information. Data security is about maintaining secrecy, which enables privacy.

Personal information is information about an identifiable individual in their personal capacity – e.g. demographic information (age, DOB, gender identity), education history, work and educational performance

Virtual work

Virtual work

Virtual work security basics

- Work only via approved services and devices
- Connect to the network via a secure connection
- Family prohibited from using devices
- Data on devices is encrypted and secured
- Printouts that go outside the office, if allowed, are handled with care (no printing of PI unless strictly necessary or with special approval)
- Work done in private, so conversations are not overheard, documents are not browsed, screens not seen

Virtual work

Network monitoring

- Endpoint monitoring and data loss prevention tools are important data security tools today, as is routine logging
- It is generally permissible, though governed by some university collective agreements
- This form of monitoring now needs to be disclosed in policy in Ontario (though Colleges are exempt)
- Reasonable transparency may help modify user behavior and shift some more risky activity onto personal devices

Online academic delivery

Online academic delivery

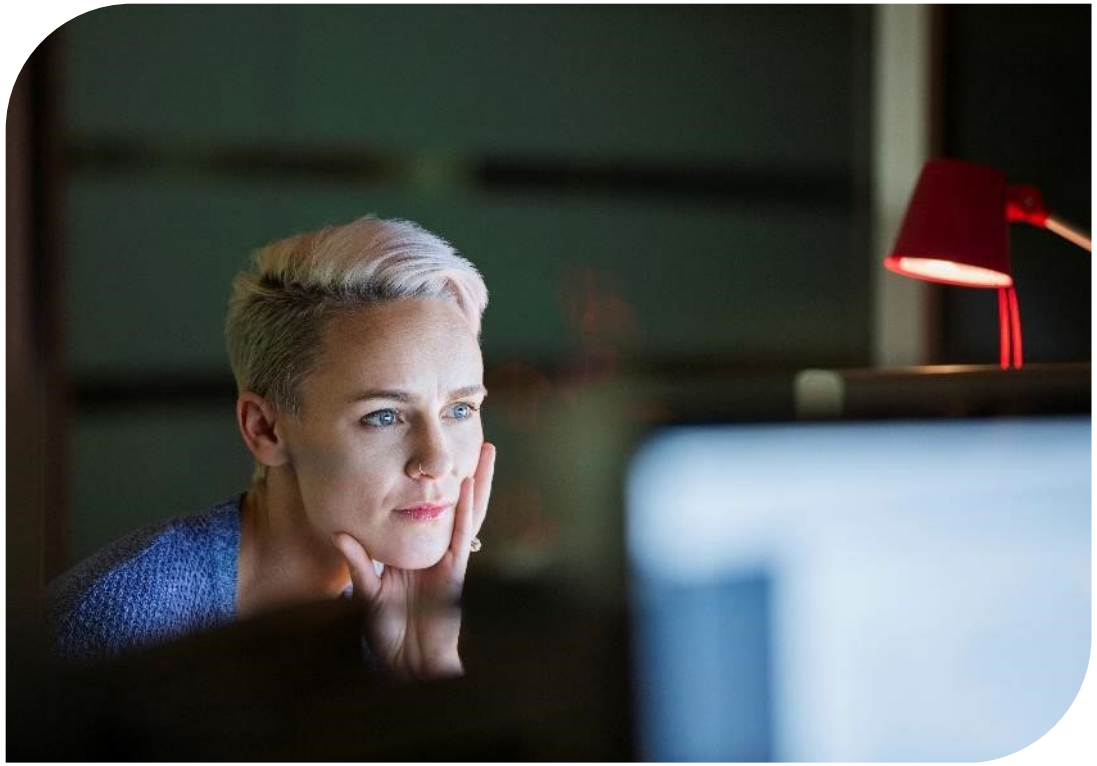
Virtual meeting privacy issues

- Cameras on or off?
  - Not a “collection” unless recording, but still a privacy issue to understand and address via guidance
  - There is a rationale requiring teacher cameras on when teaching
- Transcripts and recordings
  - For what purpose?
  - When is it not appropriate? Will it change the dynamic in the class?
  - How to give notice?
  - Who can access the transcript?
  - How long is it retained?

Online academic delivery

Online proctoring

- Classic privacy problem
  - Has a significant benefit
  - Has a privacy impact
- Given the impact, a last resort
  - Alternative means of evaluation
  - Use of test centres
- And minimize the impact
  - Give guidance to students
  - Incorporate human review
  - Minimize access
  - Minimize retention



Educational technology

Educational technology

Institution in control model

- Example – Institution subscribes to cloud based student information system
- Vendor processes information for the institution
- The institution is fully accountable to individuals and owns the records
- The instruction must be duly diligent in respect of privacy and data security
- Initiating and managing the relationship is costly

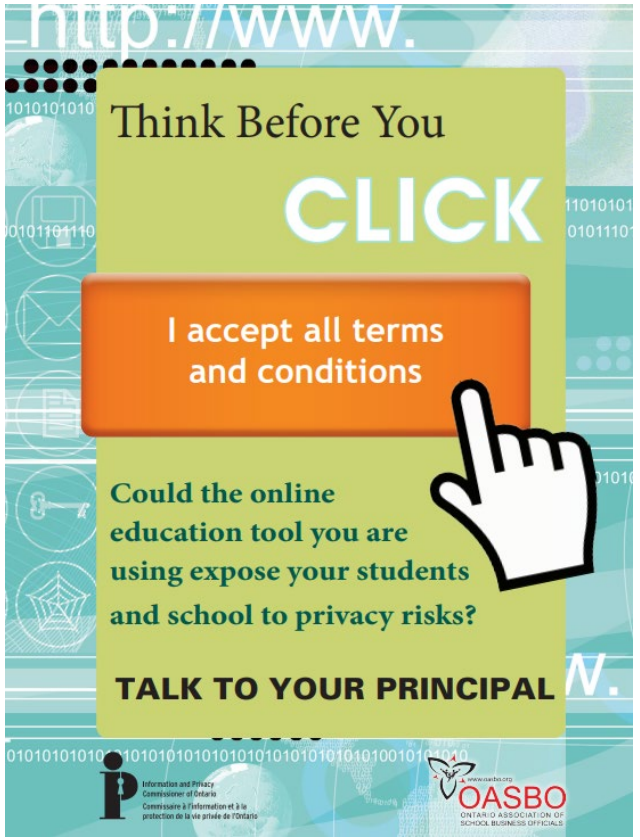
Referral model

- → *Example – teacher invites students to use a novel tool*
- → *There is an accountability, but it is indirect and invites ambiguity regarding who bears the risk and liability*
- → *Loss of control may not be appropriate – should 3Ps every be in control of our educational environment?*

Educational technology

Best practice and IPC guidance

- Establish boundaries for use of the referral model, and support professors and instructors – give them a checklist to informally assess the risk, offer counsel
  - What information will the vendor process? How sensitive is it?
  - Who is the vendor? Does it identify itself? Is it present in Canada?
  - How will the vendor use the information?
  - To whom will the vendor disclose information? Will it sell information to others?
- Provide professors and instructors with safe, institution-governed alternatives – *i.e.*, provide the basics



Cloud computing

Cloud computing

- Vendor selection diligence
- Contracting diligence
- Relationship diligence

Cloud computing

Control through contracting

- Data ownership
  - Acknowledgement
  - Export and secure disposition
- Restricted use and disclosure
  - Restrictions on subcontracting
- Data security program
  - Reasonable
  - Notice of incident
- Ongoing assurance
  - Audit right or alternative
- Promises regarding legal demands
- Compliance with applicable laws

Consider the consequences of breach and risk allocation. Are there meaningful consequences of breach? Will the vendor be liable? For how much? Should the vendor indemnify for events other than a breach?

Privacy impact assessments

Privacy Impact Assessments

- Structured methodology for assessing and addressing privacy risks
- Best practice & mitigates risk
- May result in a "no go" decision or acceptance of risk, or acceptance of risk with a mitigation plan
- Tips
  - Engage privacy office early
  - Tailor the PIA process to the risk
  - Share your PIAs
  - Focus quickly on the real issue

PERSONAL INFORMATION	COLLECTED by? from? how? when? where? why? authority?	USED by? how? when? where? why? authority?	RETAINED by? how? how long? where? why?	SECURED by? how? when? where? why?	DISCLOSED by? to? how? when? where? why? authority?	DISPOSED OF by? how? when? where? why? authority?

	How principle will be addressed	Assessment of adequacy and risk	Recommendation(s)
IV. Limiting collection[7] • Is the collection of PHI necessary? *(Consider on a data element by data element basis.)* ○ Does the hospital possess other information that will serve the purpose of the collection? • Is the collection indirect? If so, will it comply with section 36(1)?			

Managing privacy breaches

Managing privacy breaches

Breach basics

- Unauthorized use, disclosure… loss or theft
- Examples
  - Counsellor in student health snoops
  - Errant e-mail message
  - Cloud data left exposed
  - Online class recorded in breach of policy
- FIPPA – notification if there is a real risk of significant harm is customary
- PHIPA – notification of any breach is required

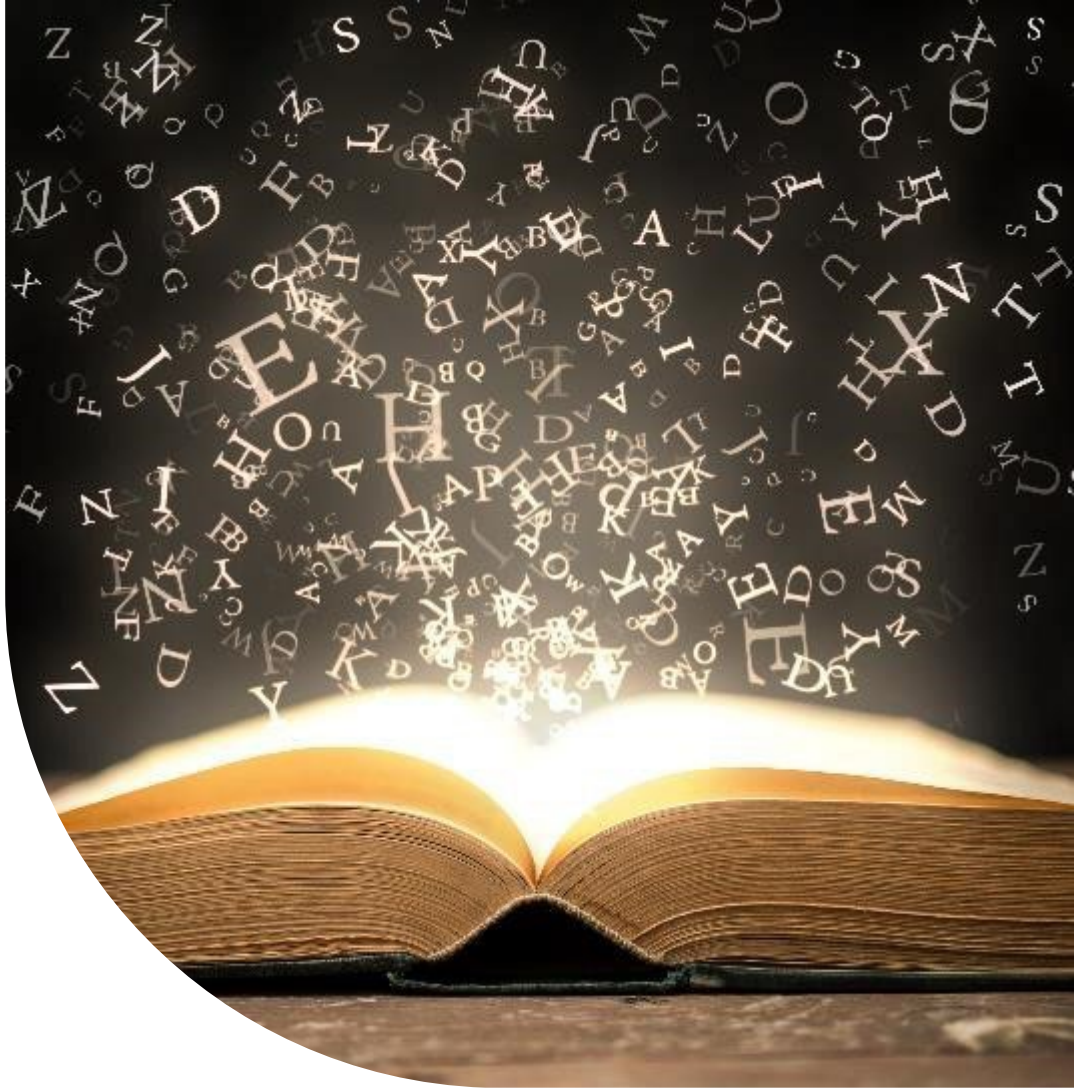
Managing privacy breaches

- Response always starts with containment – do what makes sense and get help right away
- Don’t notify without first contacting the privacy office and getting help
- Once the matter with is with the privacy office, be methodical and take the time to investigate
  - Understand the exposure
  - Understand the causal factors
- Consider who is qualified to investigate – Does the investigator have the appropriate knowledge and skill? Is the investigator independent enough?
- Then consider what might be appropriate to mitigate the risks, which may invite notification

Thank You

For more information, contact:

Dan Michaluk
Partner
416.948.6346
dmichaluk@blg.com



Borden Ladner Gervais