WELCOME

Added experience. Added clarity. Added value.

VANCOUVER     CALGARY     EDMONTON     SASKATOON     REGINA     LONDON     KITCHENER-WATERLOO     GUELPH     TORONTO     MARKHAM     MONTRÉAL

EDUCATION LAW

MORNING RECESS

Added experience. Added clarity. Added value.

Miller Thomson
lawyers | avocats
Protecting Personal Privacy in an Era of Social Media

Nadya Tymochenko
educationlaw@millerthomson.com
November 26, 2015
Introduction

• Use of Internet, social media and apps for Instructional purpose(s)
  • Enhanced communication options
  • Differentiated instruction
  • Student engagement/focus
  • Authentic audience
  • Cooperative/group learning
  • Low or no cost
Last Month: Terms and Conditions of End User Licensing Agreements ("EULA’s")

- Are they binding?
- Common terms
- Implications for users
- Implications for school boards
- Responsibility and liability
Introduction (cont.)

This Month: Protecting Personal Privacy

- Concept
- *Canadian Charter of Rights & Freedoms*
- Searches of Student Devices
- Legislative obligations to students
  - *Education Act*
  - *Municipal Freedom of Information and Protection of Privacy Act*
- Legislative obligations for profit companies
  - *Personal Information Protection and Electronic Documents Act*
- When should parental consent be sought?
SCC has recognized three distinct privacy interests:

- **territorial privacy**, acknowledging an individual’s right to be protected in the home and other places where there is a reasonable expectation of privacy;

- **physical privacy**, based on the right to personal bodily integrity; and

- **informational privacy**, grounded in the notion that personal information fundamentally belongs to the individual, and is theirs to communicate or not, as they see fit.

- *Dyment*: all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit.
Former Ontario Information and Privacy Commissioner Ann Cavoukian:

“In contrast to the ongoing work of legislators, regulators, drafters of policies and jurists who are concerned with the protection of personal information, young people willingly and paradoxically by-pass the protections put in place for their benefit and freely share all of the details and more which the law seeks to protect on their behalf.”
The need to be acknowledged online can outweigh considerations of privacy:

- 91% post a photo of themselves,
- 71% post their school name
- 71% post the city or town where they live,
- 53% post their email address,
- 20% post their cell phone number
Students & Privacy Concepts

- social media offer the illusion of privacy by:
  - identifying privacy setting;
  - personalizing a page;
  - accepting and denying requests for access;
  - posting images and information own’s choosing
  - may be copied and shared by any visitors
Students & Privacy Concepts

- Students worry about physical or territorial privacy, (their backpack; their room)
- Invasion through informational privacy and ‘big data’ occurring invisibly and remotely
- Students who have grown up with the Internet, social media, cell phones, wearable data collection devices, do not always understand right to, need for, informational privacy.
- Meaning and importance of privacy must be explicitly taught
Charter of Rights & Freedoms

*Charter* does not reference a right to informational privacy, but reflected in section 2 of the *Charter* states:

Everyone has the following fundamental freedoms:

(a) freedom of conscience and religion;

(b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;

(c) freedom of peaceful assembly; and

(d) freedom of association.
Charter rights to physical, territorial and informational privacy expressed in:

- section 7 right to life, liberty and the security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice
- section 8 right to be secure against unreasonable search or seizure
SCC recognition of informational privacy:

“In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s.8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.”
R. v. Cole

- Teacher found with child pornography (including images of student) on laptop purchased by school board for his use

- SCC found: Cole had a subjective reasonable expectation of privacy in the personal informational contents of his laptop despite the laptop being school board property.

- “Computers that are reasonably used for personal purpose – whether found in the workplace or the home – contain information that is meaningful, intimate and touching on the biographical core. Canadians may therefore reasonably expect privacy in the information contained on these computers, at least when personal use is permitted or reasonably expected.”
Case Law - R. v. Cole


- workplace policies and practices which included an assertion of board ownership of the data on the computer, as well as the hardware, diminished Mr. Cole’s expectation of privacy, but did not eliminate it.

- Court recognized that the Principal had a duty to maintain a safe school environment, therefore, reasonable power to search and seize the laptop.

- free to report information to the police.
R. v. Ward, 112 OR (3d) 321, 296 OAC 298

- the police obtained the name and address of a suspect from his Internet Service Provider (ISP) without a warrant.

- nothing preventing the ISP provider from complying with the police request for a name and address, made lawfully under Section 7(3) of the PIPEDA
Case Law – R. v. Ferron


• after arrest for jewellery store hold up police searched smart phone without warrant

• found a photo of a handgun and an unsent text message to a third person suggesting involved in the robbery
Searching Student’s Devices

- school administrator may search a student’s laptop, tablet or mobile device, provided that he or she has **reasonable grounds to believe** that the student violated a school rule
- limit the search to evidence of the breached rule
- no right to randomly review all of the student’s stored personal information
- no right to act on any other information inadvertently discovered if beyond the scope of the original search
Education Act, R.S.O. 1990, c.E. 2

• 266(2) OSR privileged for use of supervisory officers, principals, teachers and DECEs of the school for the improvement of instruction and other education of the pupil
  • not available without the written permission of the parent or guardian of the pupil or, where the pupil is an adult, the written permission of the pupil
  • preserve secrecy in respect of the content of a record that comes to the person’s knowledge

• 266.3(1) no person shall collect, use, disclose or require the production of another person’s Ontario education number;
  • breach subject to $5000 or $25,000 fine
MFIPPA – Collection of Personal Information

- Governs collection, use and disclosure of personal information in care and control of school boards
- **Does not provide a right to collect personal information by consent**

S.28(2) No person shall collect personal information unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to administration of authorized activity.
s.48(2) Every person who contravenes subsection (1) is guilty of an offence and on conviction is liable to a fine not exceeding $5,000

• students under 16 must access rights through parents

s. 54 Any right or power conferred on an individual by this Act may be exercised,

(c) if the individual is less than sixteen years of age, by a person who has lawful custody of the individual.
Educational Program

- Collection of information is limited to that which is required for educational programs
- Use of on-line tools that collect information must be monitored
- Collection of information should not be greater than required for educational instruction, assessment and evaluation
Personal Information Protection and Electronic Documents Act

- applicable to commercial enterprises in Canada
- PIPEDA provides ten privacy principles that outline the legal responsibilities of organizations
- PIPEDA framework based on the requirement that an individual have knowledge of and give consent to the collection, use and disclosure of their personal information
- personal information should be deleted once the purpose for collection, use and disclosure is complete
Consent

- *Education Act* & MFIPPA restrict collection, use and disclosure for purposes of education
- Commercial activities require consent to collection, use and disclosure of personal information
  - *Education Act* age of consent 18, or 16 or 17 if removed from care and control of parent
  - MFIPPA age of consent 16
  - PIPEDA no age of consent
Valid Consent – Students (cont.)

• the collection by third party service provider with consent of student (if capable)
• the collection by school board for educational programming purposes only
• Ontario legislation effecting school boards higher protection than PIPEDA
  • Student rights exercised through parents
• school boards should consider requiring consent from parents unless student 18 or older
Privacy Policies

• Most EULA’s contain a link to a privacy policy.

• Applies only to Provider, and not to third parties with whom Provider disclosed/sold information.

• Allow for access to personal information of User, and those whose information is stored on User’s device.

• Personal information may be used, shared and stored indefinitely.

• Not necessarily compliant with Canadian privacy laws.
School Board Process

- Privacy policy must be reviewed
- Parental consent should be sought
- **No** collection by third party because no control over the use and disclosure by third party
- Collection limited
- Use and disclosure only for service
- Anonymizing may not be sufficient
Risk

Breach of *Education Act*, MFIPPA could provide grounds for:

- Information & Privacy Complaint
- Ontario College of Teacher Complaint
- Ombudsman Complaint
Conclusion

• students have different understanding of personal informational privacy
• case law allows for limited right to search devices
• legislation protects personal privacy but need to review privacy policy because commercial activity based on consent