Access and Privacy: IPC Resources for Educators and Students

Fred Carter
Senior Policy & Technology Advisor

MISA Northeastern Professional Network
Privacy and Information Management Symposium

Tuesday 25 April 2017

Overview

About Us

Educational Tools

Online Educational Services

Privacy Impact Assessments (PIAs)

Cloud Computing Guidance

Questions?

Office of the Information and Privacy Commissioner of Ontario (IPC)

What we do:

- Provide an **independent** review of provincial and municipal government and public sector decisions and practices concerning access and privacy
- Oversee **compliance** with provincial and municipal access and privacy legislation
- Conduct **research** and deliver **education** and guidance on access and privacy issues

Ontario Access and Privacy Laws

- The *Freedom of Information and Protection of Privacy Act (FIPPA)*
    - applies to over 300 provincial institutions such as ministries, provincial agencies, boards and commissions, as well as community colleges and universities
- **The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)***
    - **applies to over 1,200 municipal institutions such as municipalities, police services boards, school boards, conservation authorities and transit commissions**
- The *Personal Health Information Protection Act (PHIPA)*
    - covers individuals and organizations in Ontario that are involved in the delivery of health care services, including hospitals, pharmacies, laboratories and health care providers such as doctors, dentists and nurses

Privacy Obligations under M/*FIPPA*

Collection, use, disclosure rules

No **collection** unless

- authorized by statute
- used for law enforcement or
- necessary to lawfully authorized activity

Must have a legitimate reason for collecting personal information, such as requiring a birth certificate to issue a driver's license

No **use** unless

- purpose collected
- consistent purpose
- written consent

Cannot use information from the birth registry to send out birthday cards

No **disclosure** unless

- consent
- consistent purpose
- comply with legislation
- law enforcement
- health or safety
- compassionate reasons

Video capturing evidence of a crime can be shared with police, even if it contains personal information

Educational Tools

Grade 5 resources

Grade 10 resources

Grade 11 resources

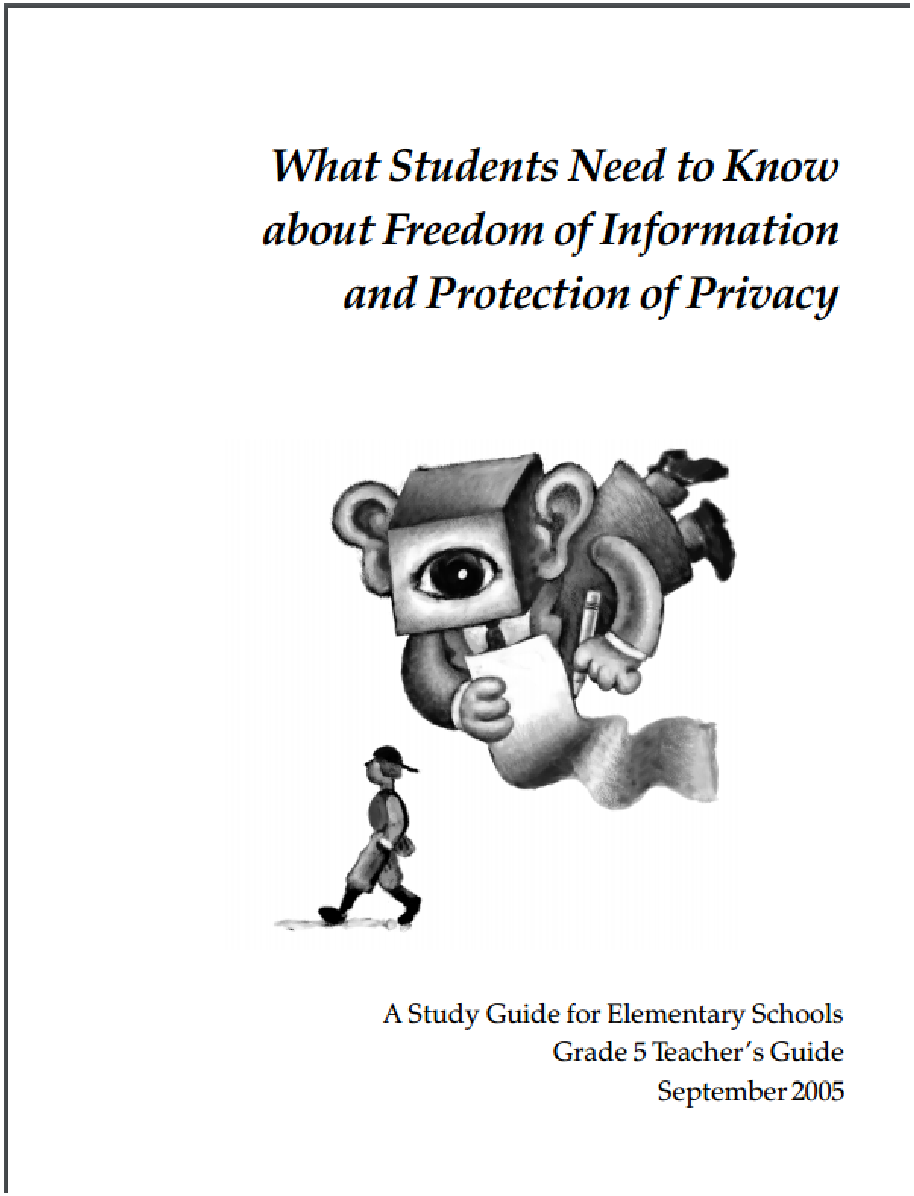
Educational Materials for Youth

Approach Taken

Other Initiatives

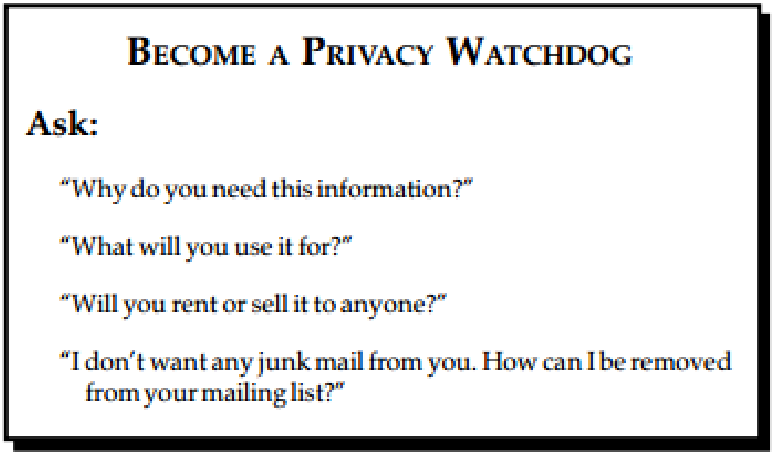
Study Guide for Elementary Schools: Grade 5 Teacher's Guide

Grade 5 students
(ages 10-11 years)



What Students Need to Know
about Freedom of Information
and Protection of Privacy

A Study Guide for Elementary Schools
Grade 5 Teacher's Guide
September 2005



Become a Privacy Watchdog

Ask:

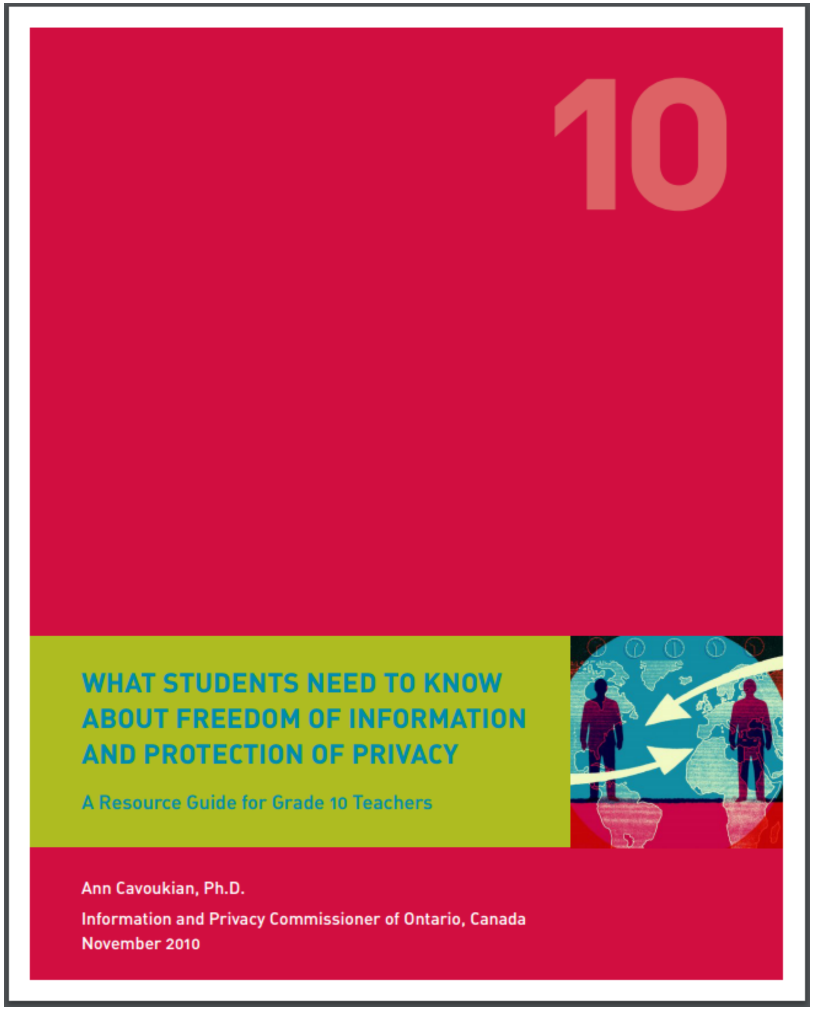
"Why do you need this information?"

"What will you use it for?"

"Will you rent or sell it to anyone?"

"I don't want any junk mail from you. How can I be removed from your mailing list?"

www.ipc.on.ca/wp-content/uploads/Resources/up-1grade_5.pdf



10

WHAT STUDENTS NEED TO KNOW ABOUT FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

A Resource Guide for Grade 10 Teachers

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario, Canada
November 2010

What Students Need to Know: A Resource guide for Grade 10 Teachers

Grade 10 students
(ages 15-16 years)

INFORMATIONAL PRIVACY

consisting of limited access to information, confidentiality, secrecy, anonymity and data protection

PHYSICAL PRIVACY

consisting of limited access to persons, possessions and personal property

DECISIONAL PRIVACY

consisting of decision-making about families, religion and health

PROPRIETARY PRIVACY

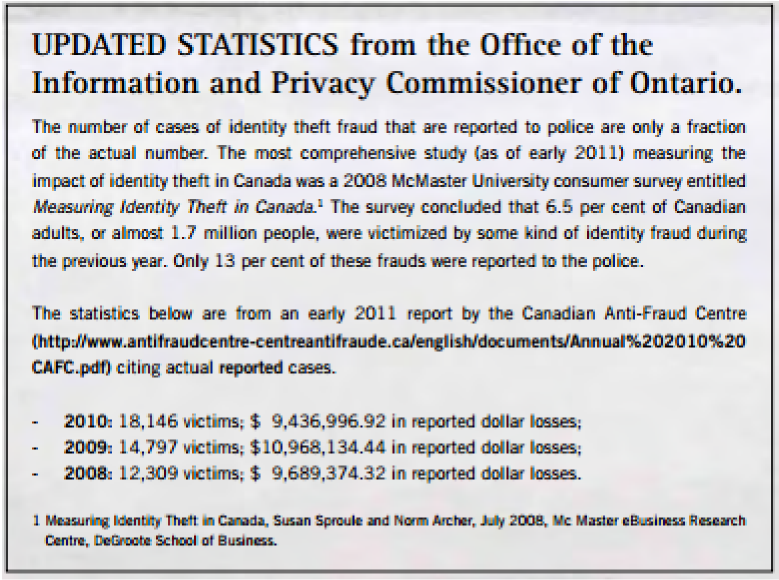
consisting of control over the attributes of personal identity.

www.ipc.on.ca/wp-content/uploads/Resources/Grade_10_web-e.pdf

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

What Students Need to Know: A Resource guide for Grade 11-12 Teachers

Grade 11-12 students
(ages 16-18 years)



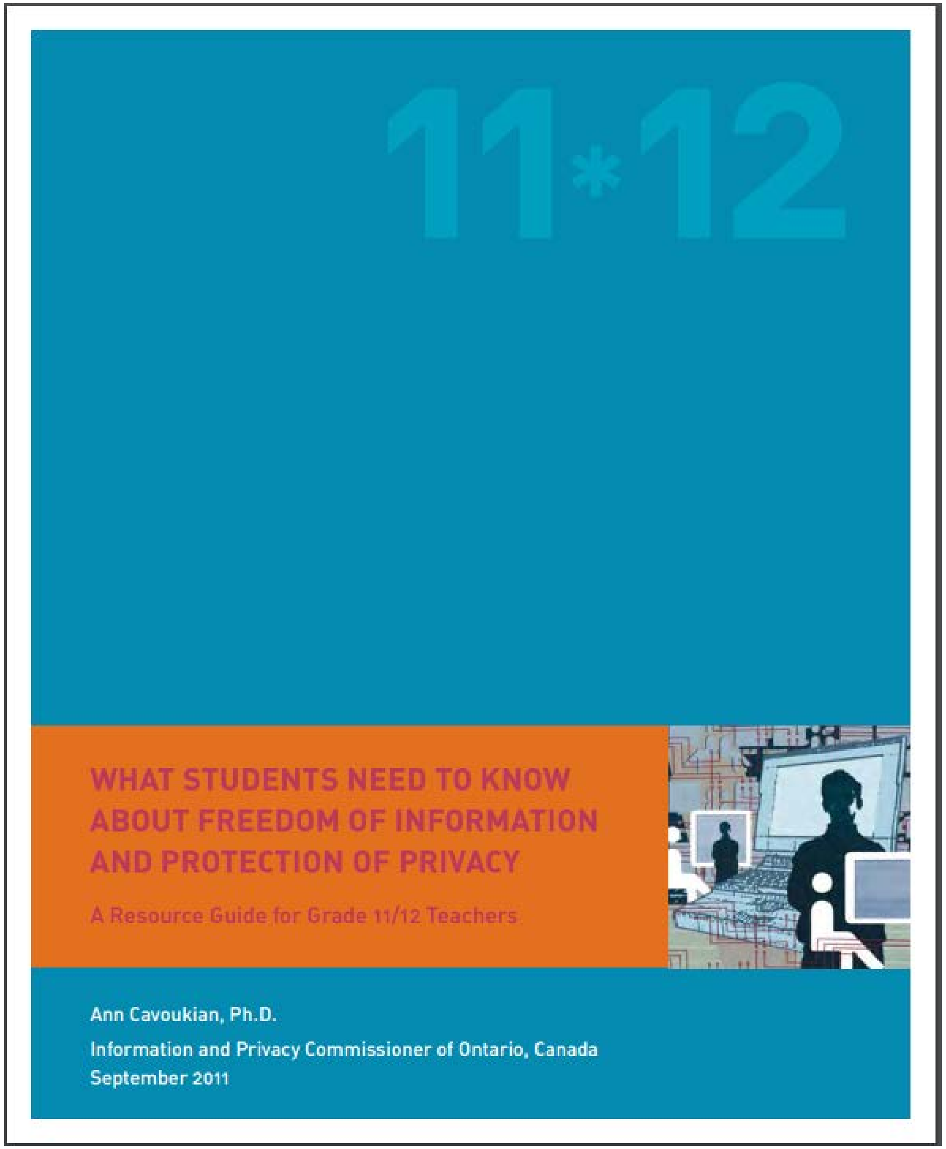
UPDATED STATISTICS from the Office of the Information and Privacy Commissioner of Ontario.

The number of cases of identity theft fraud that are reported to police are only a fraction of the actual number. The most comprehensive study (as of early 2011) measuring the impact of identity theft in Canada was a 2008 McMaster University consumer survey entitled *Measuring Identity Theft in Canada.*[1] The survey concluded that 6.5 per cent of Canadian adults, or almost 1.7 million people, were victimized by some kind of identity fraud during the previous year. Only 13 per cent of these frauds were reported to the police.

The statistics below are from an early 2011 report by the Canadian Anti-Fraud Centre (http://www.antifraudcentre-centreantifraude.ca/english/documents/Annual%202010%20CAFC.pdf) citing actual reported cases.

- **2010:** 18,146 victims; $ 9,436,996.92 in reported dollar losses;
- **2009:** 14,797 victims; $10,968,134.44 in reported dollar losses;
- **2008:** 12,309 victims; $ 9,689,374.32 in reported dollar losses.

[1] Measuring Identity Theft in Canada, Susan Sproule and Norm Archer, July 2008, Mc Master eBusiness Research Centre, DeGroote School of Business.



11*12

WHAT STUDENTS NEED TO KNOW ABOUT FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

A Resource Guide for Grade 11/12 Teachers

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario, Canada
September 2011

www.ipc.on.ca/wp-content/uploads/Resources/Grade_11-12_Resource_Guide.pdf

Educational Materials for Youth

- Collaborative Approach:
  - Frontline teachers participated in the development of our educational materials
  - School boards that oversee public schools in Ontario participated by distributing guidance

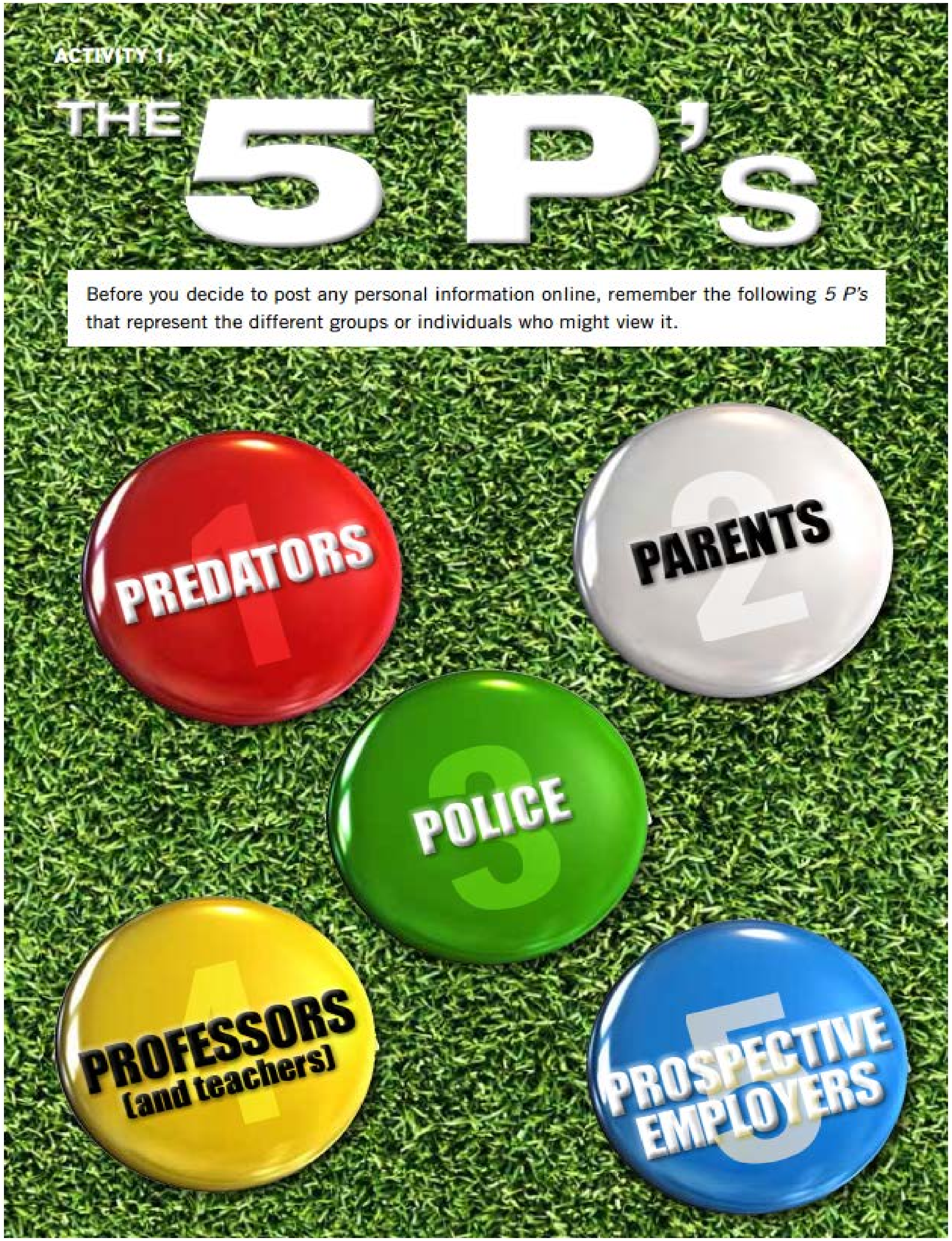
- Seamless Integration
  - Materials were based on the curriculum standards required by the Ministry of Education to allow them to seamlessly join existing teaching plans
  - Lessons based on existing plans in use by school boards
  - Teachers do not require additional training in order to teach this material

Approach Taken

- Separate materials developed based on age group.
- Variety of learning tools, including:
    - Powerpoint presentations to be given by teachers
    - Online research activities
        - For example, “webquests” where students visit specific websites to find privacy policies and information
        - Videos shown in class
        - Quizzes
        - Quick reference infographics
        - Group discussion aids
        - Case studies
        - Discussion aids around articles that relate to privacy in the news

Infographics:

- Easy to remember list of potential viewers of online content
- Reminder to kids that online posts are not private and can be seen by the wrong people
- Focus on thinking before you post



ACTIVITY 1:

THE 5 P'S

Before you decide to post any personal information online, remember the following *5 P's* that represent the different groups or individuals who might view it.

1 PREDATORS

2 PARENTS

3 POLICE

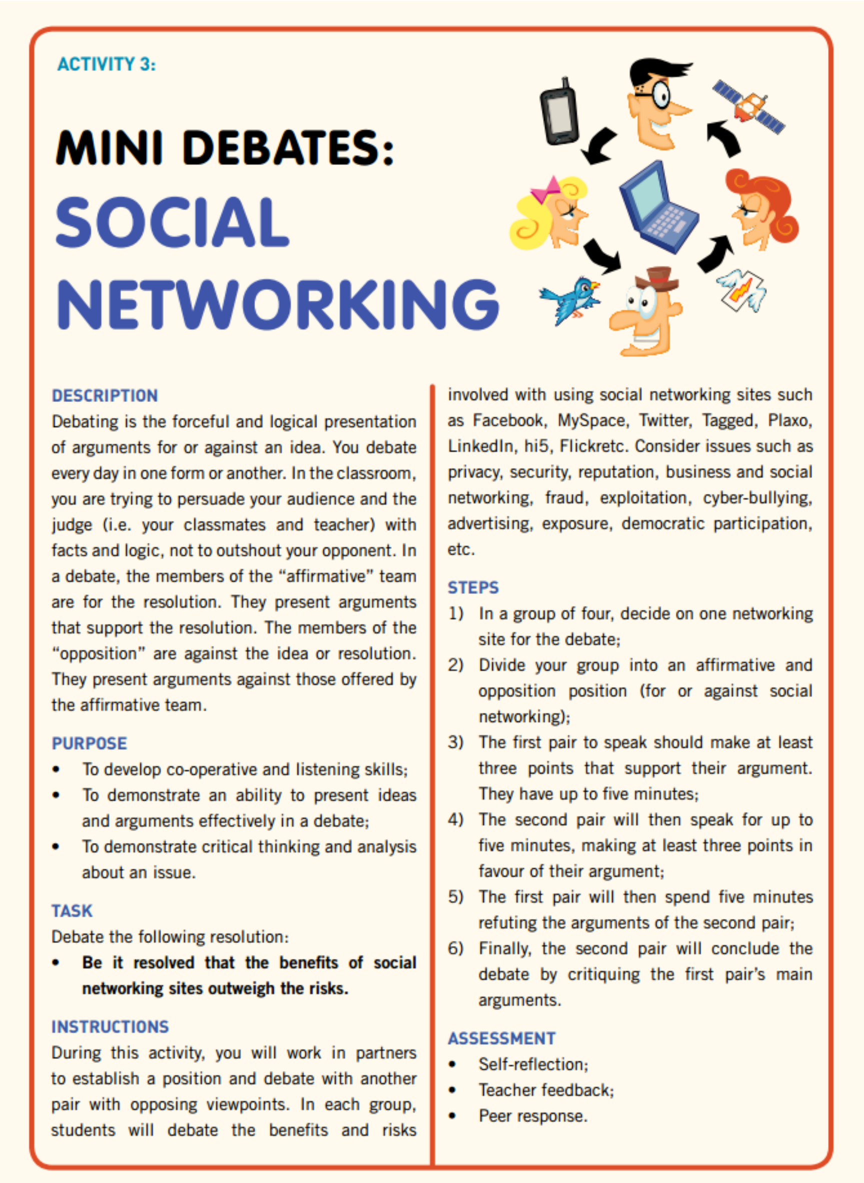
4 PROFESSORS (and teachers)

5 PROSPECTIVE EMPLOYERS

Debate Exercises:

- Students work in small teams to assess and debate the merits of various social networking platforms

- Students independently consider issues such as privacy, security, reputation and cyber-bullying, while simultaneously considering the benefits of using social networks



ACTIVITY 3:

MINI DEBATES: SOCIAL NETWORKING

DESCRIPTION

Debating is the forceful and logical presentation of arguments for or against an idea. You debate every day in one form or another. In the classroom, you are trying to persuade your audience and the judge (i.e. your classmates and teacher) with facts and logic, not to outshout your opponent. In a debate, the members of the "affirmative" team are for the resolution. They present arguments that support the resolution. The members of the "opposition" are against the idea or resolution. They present arguments against those offered by the affirmative team.

PURPOSE

- To develop co-operative and listening skills;
- To demonstrate an ability to present ideas and arguments effectively in a debate;
- To demonstrate critical thinking and analysis about an issue.

TASK

Debate the following resolution:

- **Be it resolved that the benefits of social networking sites outweigh the risks.**

INSTRUCTIONS

During this activity, you will work in partners to establish a position and debate with another pair with opposing viewpoints. In each group, students will debate the benefits and risks involved with using social networking sites such as Facebook, MySpace, Twitter, Tagged, Plaxo, LinkedIn, hi5, Flickretc. Consider issues such as privacy, security, reputation, business and social networking, fraud, exploitation, cyber-bullying, advertising, exposure, democratic participation, etc.

STEPS

1) In a group of four, decide on one networking site for the debate;
2) Divide your group into an affirmative and opposition position (for or against social networking);
3) The first pair to speak should make at least three points that support their argument. They have up to five minutes;
4) The second pair will then speak for up to five minutes, making at least three points in favour of their argument;
5) The first pair will then spend five minutes refuting the arguments of the second pair;
6) Finally, the second pair will conclude the debate by critiquing the first pair's main arguments.

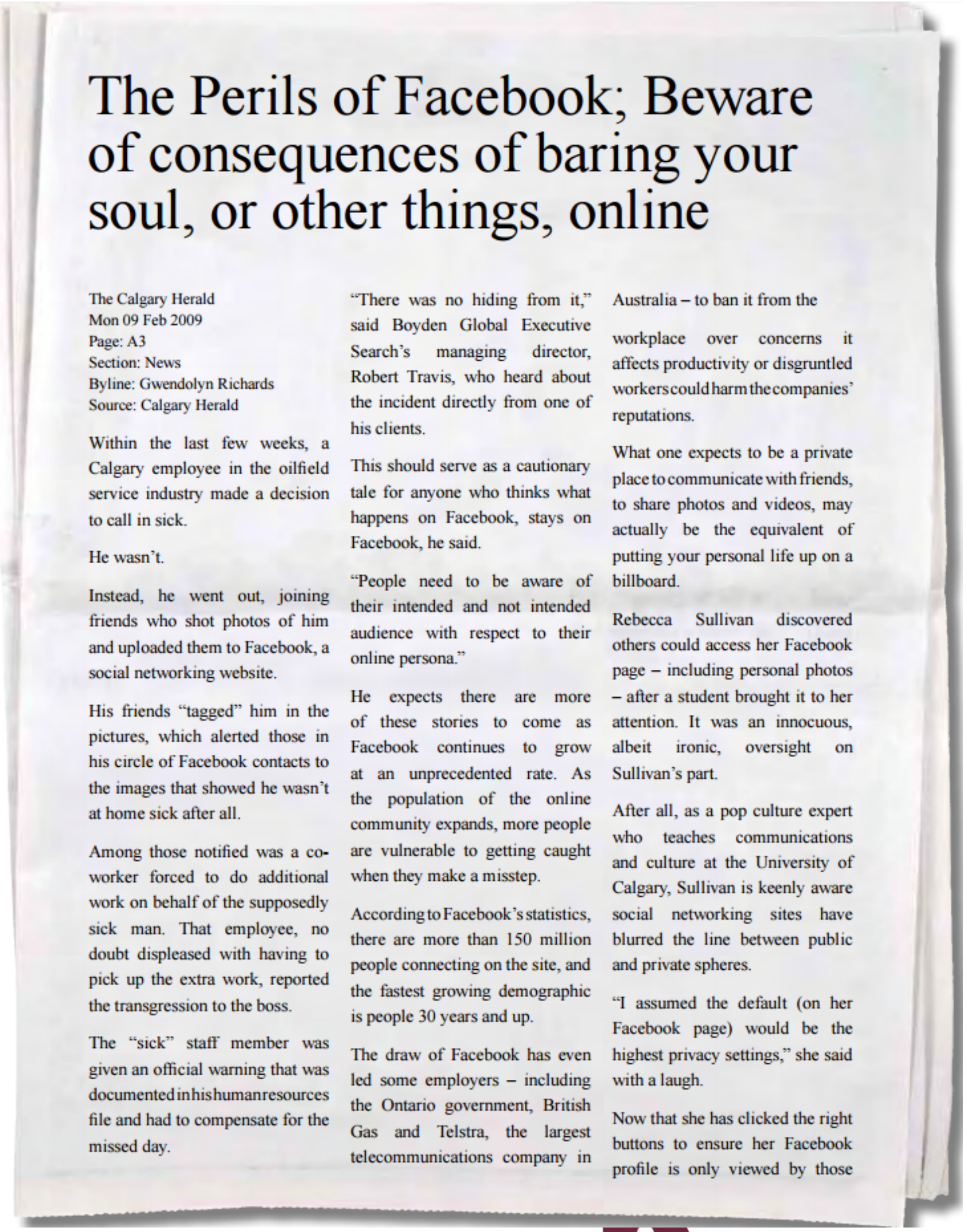
ASSESSMENT

- Self-reflection;
- Teacher feedback;
- Peer response.

News Articles

- Students are provided with real news articles dealing with the potential consequences of revealing personal information online

- Students are invited to discuss the articles and consider their own use of social media and the potential impacts to reputation and privacy



The Perils of Facebook; Beware of consequences of baring your soul, or other things, online

The Calgary Herald
Mon 09 Feb 2009
Page: A3
Section: News
Byline: Gwendolyn Richards
Source: Calgary Herald

Within the last few weeks, a Calgary employee in the oilfield service industry made a decision to call in sick.

He wasn't.

Instead, he went out, joining friends who shot photos of him and uploaded them to Facebook, a social networking website.

His friends "tagged" him in the pictures, which alerted those in his circle of Facebook contacts to the images that showed he wasn't at home sick after all.

Among those notified was a co-worker forced to do additional work on behalf of the supposedly sick man. That employee, no doubt displeased with having to pick up the extra work, reported the transgression to the boss.

The "sick" staff member was given an official warning that was documented in his human resources file and had to compensate for the missed day.

"There was no hiding from it," said Boyden Global Executive Search's managing director, Robert Travis, who heard about the incident directly from one of his clients.

This should serve as a cautionary tale for anyone who thinks what happens on Facebook, stays on Facebook, he said.

"People need to be aware of their intended and not intended audience with respect to their online persona."

He expects there are more of these stories to come as Facebook continues to grow at an unprecedented rate. As the population of the online community expands, more people are vulnerable to getting caught when they make a misstep.

According to Facebook's statistics, there are more than 150 million people connecting on the site, and the fastest growing demographic is people 30 years and up.

The draw of Facebook has even led some employers – including the Ontario government, British Gas and Telstra, the largest telecommunications company in Australia – to ban it from the workplace over concerns it affects productivity or disgruntled workers could harm the companies' reputations.

What one expects to be a private place to communicate with friends, to share photos and videos, may actually be the equivalent of putting your personal life up on a billboard.

Rebecca Sullivan discovered others could access her Facebook page – including personal photos – after a student brought it to her attention. It was an innocuous, albeit ironic, oversight on Sullivan's part.

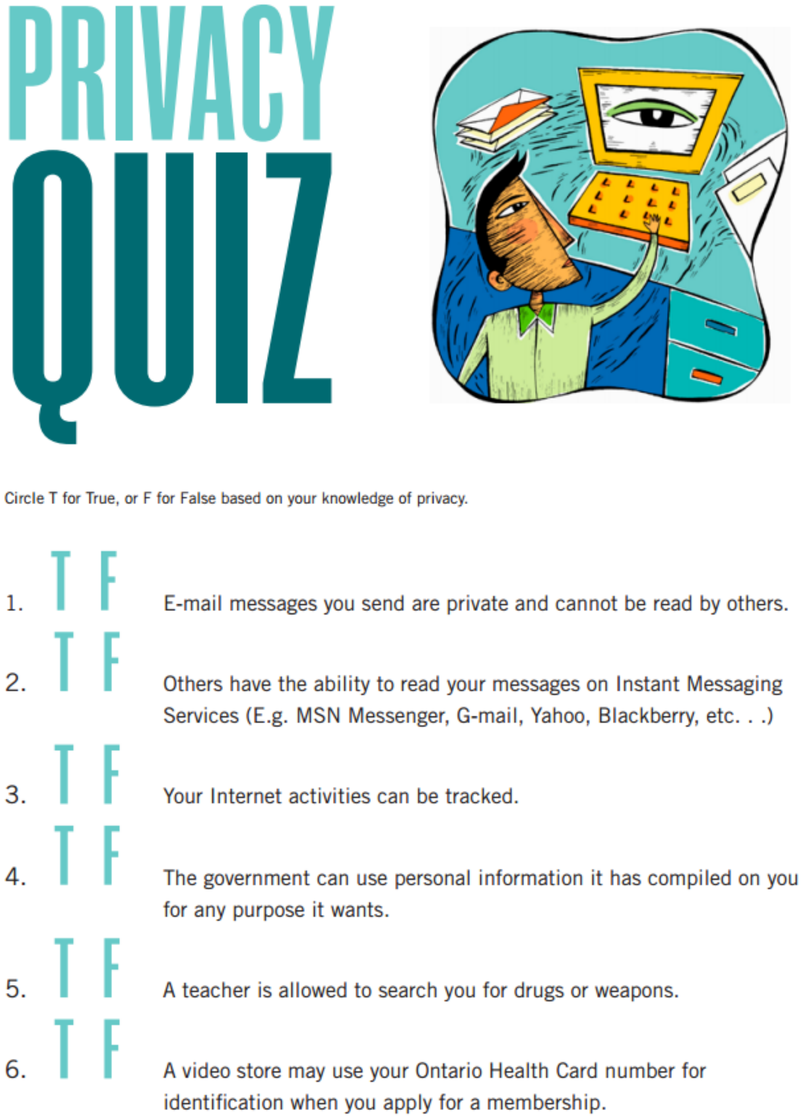
After all, as a pop culture expert who teaches communications and culture at the University of Calgary, Sullivan is keenly aware social networking sites have blurred the line between public and private spheres.

"I assumed the default (on her Facebook page) would be the highest privacy settings," she said with a laugh.

Now that she has clicked the right buttons to ensure her Facebook profile is only viewed by those

Short Quizzes

- Quizzes vary in complexity based on target age groups
- The questions have been designed to start conversations on privacy rights and technology



PRIVACY QUIZ

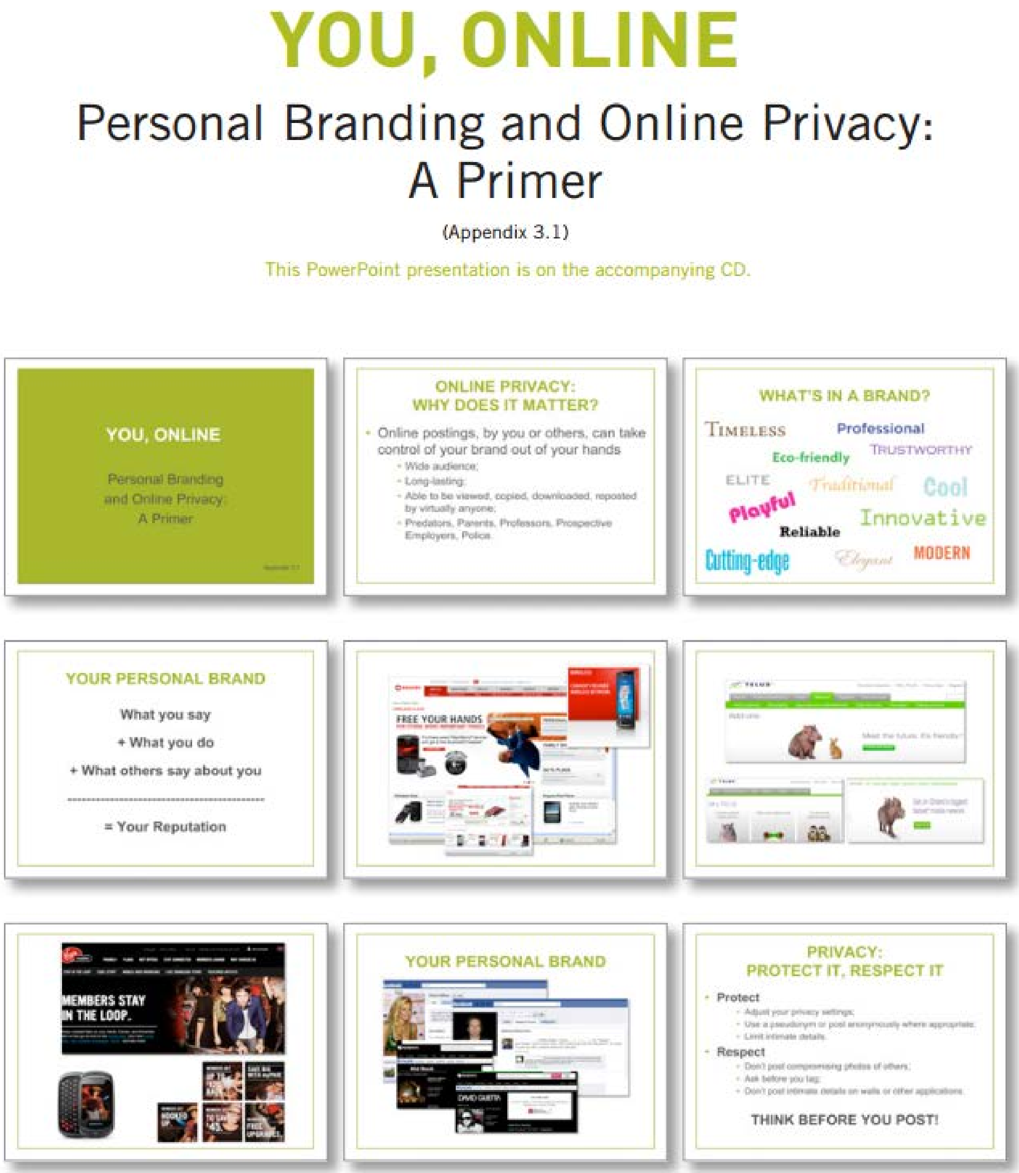
Circle T for True, or F for False based on your knowledge of privacy.

1. T F E-mail messages you send are private and cannot be read by others.
2. T F Others have the ability to read your messages on Instant Messaging Services (E.g. MSN Messenger, G-mail, Yahoo, Blackberry, etc. . .)
3. T F Your Internet activities can be tracked.
4. T F The government can use personal information it has compiled on you for any purpose it wants.
5. T F A teacher is allowed to search you for drugs or weapons.
6. T F A video store may use your Ontario Health Card number for identification when you apply for a membership.

Powerpoint Presentations

- Slide decks provide teachers with easy to use lecture tools that focus on issues like online privacy and reputation

- Presentations use numerous examples from websites and social media to help students understand the impact of online privacy on their lives



YOU, ONLINE

Personal Branding and Online Privacy:
A Primer

(Appendix 3.1)

This PowerPoint presentation is on the accompanying CD.

YOU, ONLINE

Personal Branding
and Online Privacy:
A Primer

ONLINE PRIVACY:
WHY DOES IT MATTER?

- Online postings, by you or others, can take control of your brand out of your hands
  - Wide audience;
  - Long-lasting;
  - Able to be viewed, copied, downloaded, reposted by virtually anyone;
  - Predators, Parents, Professors, Prospective Employers, Police

WHAT'S IN A BRAND?

YOUR PERSONAL BRAND

What you say

+ What you do

+ What others say about you

= Your Reputation

YOUR PERSONAL BRAND

PRIVACY:
PROTECT IT, RESPECT IT

- Protect
  - Adjust your privacy settings;
  - Use a pseudonym or post anonymously where appropriate;
  - Limit intimate details.
- Respect
  - Don't post compromising photos of others;
  - Ask before you tag;
  - Don't post intimate details on walls or other applications.

THINK BEFORE YOU POST!

Online Educational Services

Collaborative work:

Brochure

Posters

November workshop

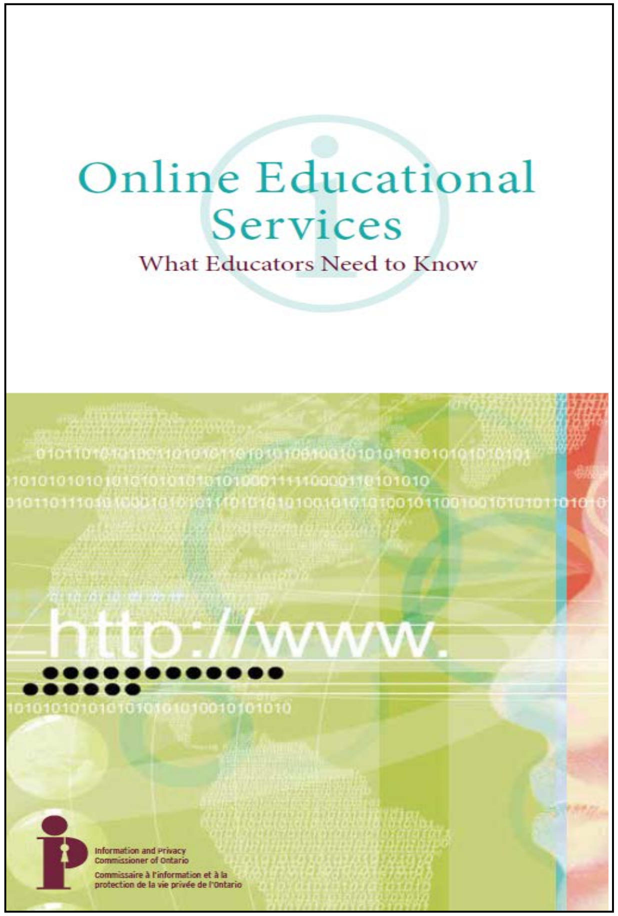
Decision-Tree Tool

2017 GPEN Sweep

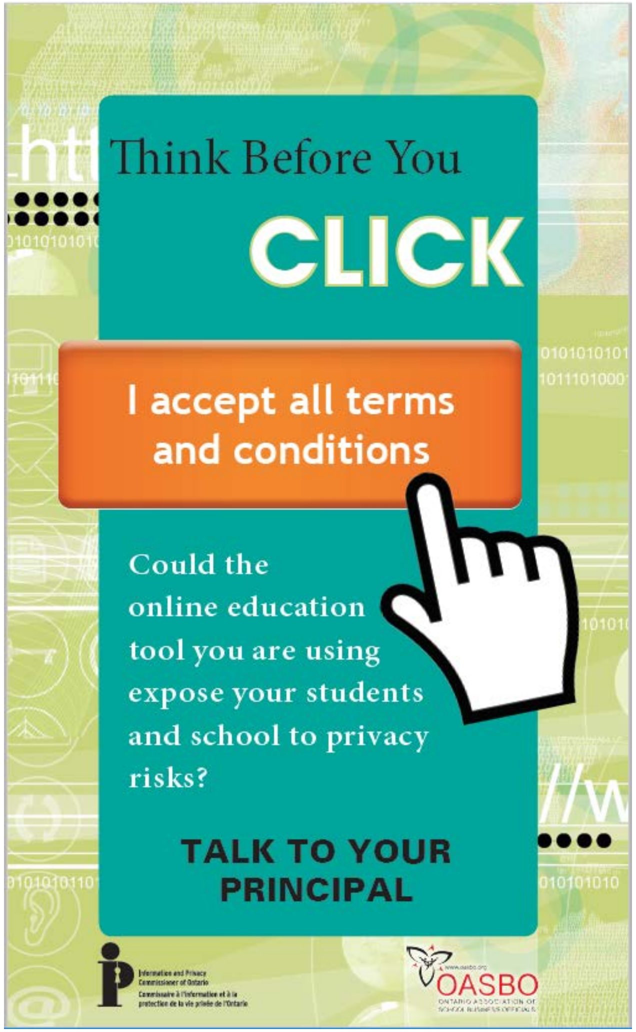
Other initiatives

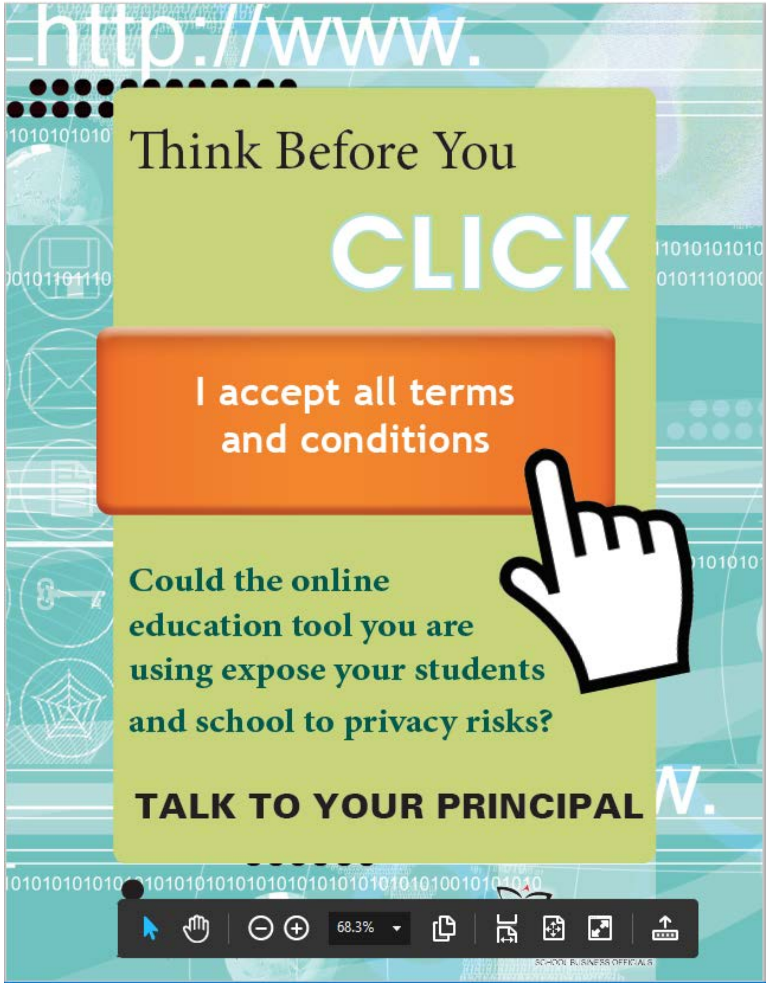
Teachers Must Consider Privacy Before Using Online Services

- Educators use online educational services for learning, communication and evaluation
- While innovative and inexpensive, they may risk privacy of students and their families
- School boards must ensure online services used by teachers are compliant with privacy laws
- IPC and Ontario Association of School Board Officials (OASBO) created fact sheet about privacy risks of online educational services


Online Educational Services
What Educators Need to Know
http://www.
Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Posters


Think Before You
CLICK
I accept all terms and conditions
Could the online education tool you are using expose your students and school to privacy risks?
TALK TO YOUR PRINCIPAL
Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario
www.oasbo.org
OASBO
ONTARIO ASSOCIATION OF SCHOOL BUSINESS OFFICIALS


http://www.
Think Before You
CLICK
I accept all terms and conditions
Could the online education tool you are using expose your students and school to privacy risks?
TALK TO YOUR PRINCIPAL
68.3%
SCHOOL BUSINESS OFFICIALS

www.ipc.on.ca/privacy/data-and-technology-management/oes/

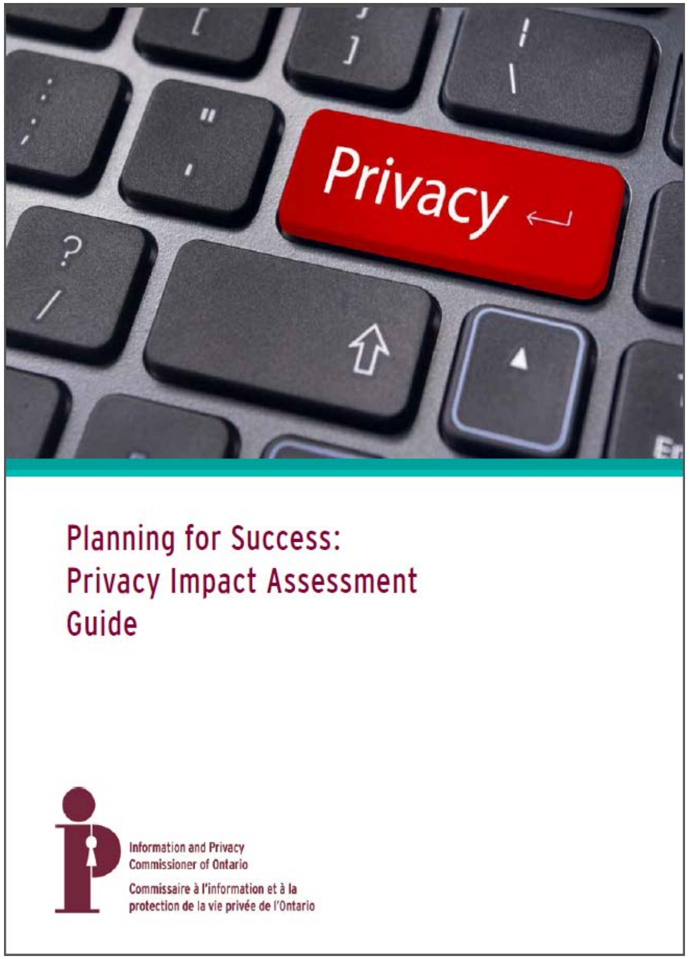
Privacy Impact Assessments (PIAs)

- Longstanding IPC interest in PETs, privacy-enhancing architectures, proactive risk reduction
- PHIPA PIA Guide (2005)
- Process/tool to **identify and analyze privacy risks** when changing or developing programs or systems
- Due diligence exercise; document decisions
- Useful during Reviews, Complaints, Investigations
- Trend: proactive assurance and attestation of information management practices.

Privacy Impact Assessments

- IPC reviewed current state of the art
- OPS PIA approach was the chosen template/model
- Need to establish common baseline
- Requirements for PIA Guide:
  - Short (< 15 pages)
  - Readable (4 major steps)
  - Usable (include practical tools)
  - Compatible with existing methods and processes

Privacy Impact Assessments



Planning for Success:
Privacy Impact Assessment
Guide

Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

PIA Guide

- Tool to identify privacy effects, mitigate risks, of a given project
- Widely recognized as a best practice
- Simplified 4-step methodology with tools
- Basis for developing internal PIA policies and procedures

Download at: https://goo.gl/9gM1x6

PIA Methodology and Tools

Key Steps	Tools
1. Preliminary Analysis Is personal Information involved?	**Appendix A: Questionnaire**
2. Project Analysis Gather project info, people and resources	**Appendix B: Questionnaire**
3. Privacy Analysis Identify and mitigate risks	**Appendix C: Checklist**
4. PIA Report Document findings, get approval, proceed	**Appendix D: Template**

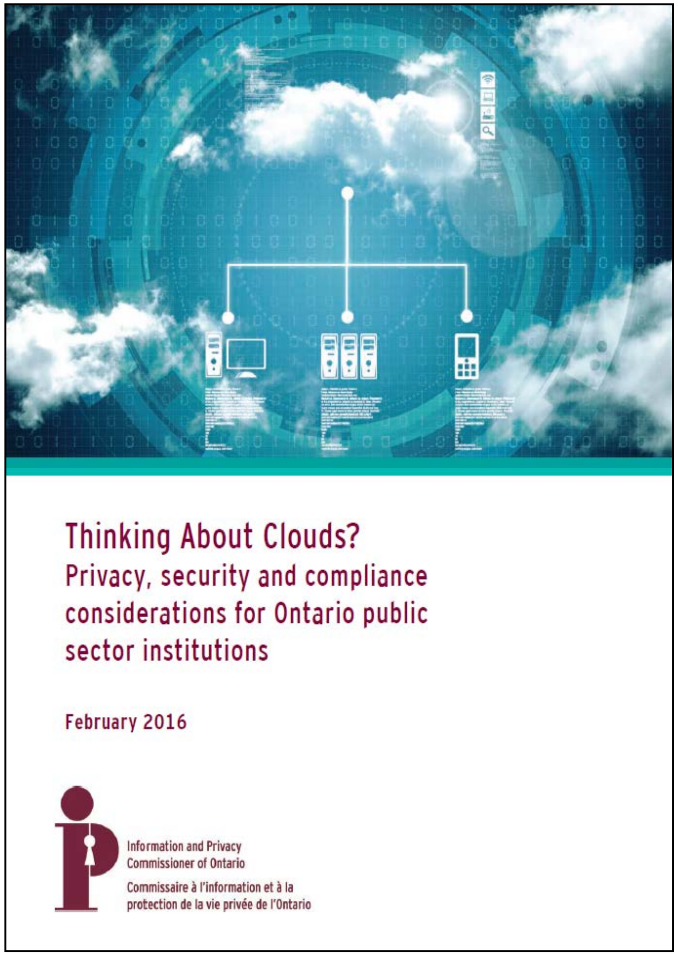
Downloadable Worksheet containing all Appendices: https://goo.gl/aRS8I4

Cloud Computing

- Significant computing development / trend
- Hot-button political, legal, economic and privacy issue
- Numerous inquiries and requests re:
  - Use of public clouds
  - Cloud security
  - Territoriality
- Uncertainty, confusion about using cloud-computing services

Cloud Computing Guidance

- Evaluate whether cloud computing services are suitable
- Identify risks associated with using cloud computing
- Outline strategies to mitigate risks



Thinking About Clouds?

Privacy, security and compliance considerations for Ontario public sector institutions

February 2016

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Cloud Computing
Risks and Mitigation Strategies

Risks

- Unauthorized Processing and Secondary Uses
- Covert Surveillance
- Insider Threats
- Data Permanence
- Loss of Access
- Identifying Applicable Law
- Audit
- Inability to negotiate terms of service

Risk Mitigation Strategies

- Understand Your Legal and Policy Obligations
- Conduct a PIA and TRA
- Minimize PI
- Know Your Cloud Service Provider
- Negotiate Comprehensive and Enforceable Contracts
- Consider Applicable Standards
- Incident Management Plan

The IPC’S Open Door Policy

- Achieving the kind of balance we are striving for is not possible without the involvement of other agencies and stakeholders
- The IPC has an **open door policy** for any Ontario institution considering programs which may impact privacy
- We believe that the vast majority of privacy challenges can be addressed through collaboration
- Appropriate privacy protections can be developed and must be implemented
- The key is to address privacy concerns from the outset

QUESTIONS

???

How to Contact Us

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
TDD/TTY: 416-325-7539
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965

Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario