



***Youth Online:
Beware of the "5Ps"
When Using Social Networks***

**31st International
Conference
of Data Protection and
Privacy Commissioners
Madrid, Spain
November 5, 2009**

**Ann Cavoukian, Ph.D.
Information & Privacy
Commissioner
Ontario, Canada**



Presentation Outline

➤ Health

*Personal Health Information
Protection Act (PHIPA)*

➤ Education

*On-line Social Networking:
Beware of the “5Ps”*



*Personal Health
Information Act
PHIPA*



Personal Health Information Protection Act (PHIPA)

- Applies to organizations and individuals involved in the delivery of health care services (both public and private sector);
- The only health sector privacy legislation in Canada based on consent: implied consent within healthcare providers' "circle of care," otherwise, express consent;
- The only health sector privacy legislation that was declared to be substantially similar to Canada's federal private sector law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).



PHIPA as a Model for Health Research

- U.S. Institute of Medicine, in its publication: *Beyond the HIPAA Privacy Rule, Enhancing Privacy, Improving Health Through Research* – concluded that the existing U.S. *HIPAA* Privacy Rule does not sufficiently protect privacy;
- Pointed to Ontario's *Personal Health Information Protection Act (PHIPA)* as a model framework for developing a new approach in the United States.



Online Social Networks



Our Work with Facebook

- In 2005, we were first approached by senior executives from Facebook seeking input on their privacy measures;
- This work included holding a student focus group to determine if and how students are aware of their privacy options;
- From our interaction with these students, we made the surprising discovery that none of them had set their privacy filters, and most were completely unaware of the privacy options available to them;
- We felt it was critical to get the message out that while social networking websites can be addictive, they can also be dangerous;
- We wanted these students and others to understand that when they choose to connect with their friends through a social networking website, they must remember that it is they who are ultimately responsible for determining what information they share with others.



Talking to Youth: Beware of *the 5 Ps*

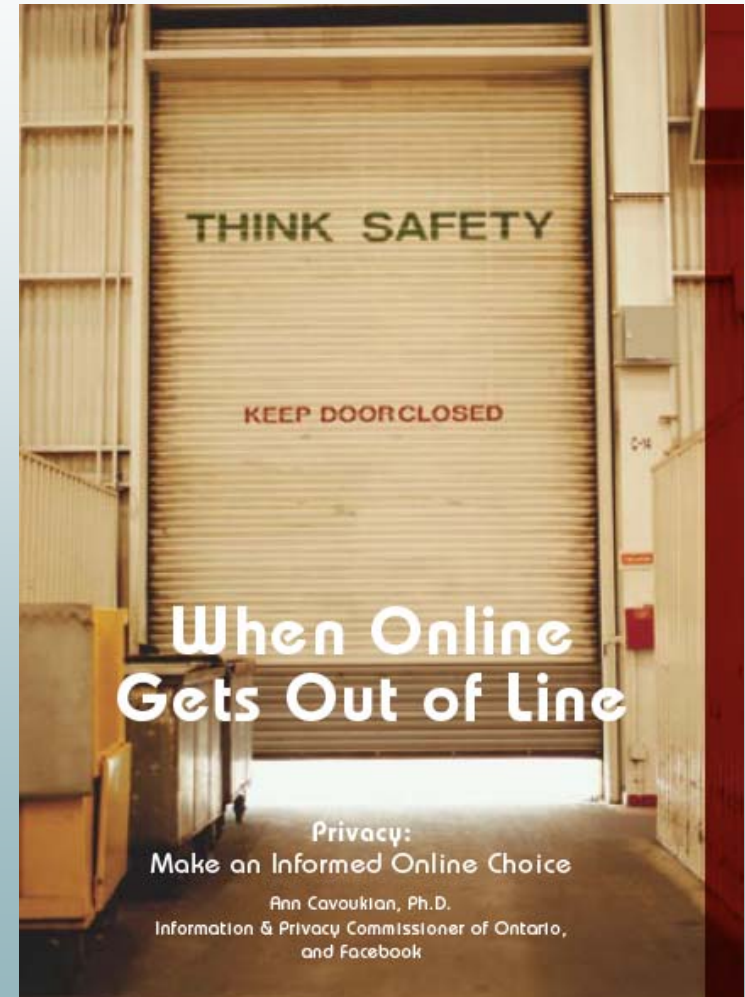
➤ I have spoken at a number of schools in my attempt to reach out to students regarding how they can stay safe, and in control, while online. My main message to them has been to always be aware of the 5 Ps:

- 1. Predators**
- 2. Parents**
- 3. Professors (Teachers)**
- 4. Prospective employers**
- 5. Police**



IPC Brochure: *When Online Gets Out of Line*

- University and high school students need to consider all the potential implications before posting personal information to online social networking sites;
- It is important that students take the time to make informed choices about the site they use, the information they post and those with whom they choose to share their information;
- Going on “automatic pilot” online is a bad idea. *Always think before you click!*






IPC Facebook Tipsheet

How to Protect Your Privacy on Facebook

- When you sign up as a user of Facebook, the default settings allow all other Facebook users to find you in searches;
- By default, your name and thumbnail profile picture can also be found on public search engines. Facebook has selected these settings based on what it believes most users want, but you can always change them to restrict access to your information, as you see fit.



information and privacy
commission of canada

How to Protect your Privacy on Facebook

When you sign up as a user of Facebook, the default settings allow all other Facebook users to find you in searches. However, only those you have confirmed as friends or who share a network with you have access to your full profile. By default, your name and thumbnail profile picture can also be found on public search engines. Facebook has selected these settings based on what it believes most users want, but you can always change them to restrict access to your information, as you see fit. Therefore, you can change the default settings to restrict access to your profile. Under the current setting, only your friends, their friends and the people on your networks can see your profile. If you download Facebook Platform third-party applications into your profile, some of your information may be shared (see section on Applications below). It is important to explore these default settings, to adjust the privacy settings to that with which you are comfortable.

It's easy to change the default settings. Once you sign in, click on "privacy" on the top-right side of the screen or the bottom-right side, or visit <http://Facebook.com/privacy>. The Privacy Overview menu has four categories in which you can determine the degree of privacy you would like. You can click on each heading to access the page on which you can make your changes. Privacy settings can be customized to exclude or include specific friends or lists of friends. Creating these lists is done in the Friends section of the site by clicking on the Make a New List button and following the step-by-step instructions.

Profile: This page contains two tabs, each with numerous individual controls for who can see aspects of your profile. On the Basic tab are controls for your entire profile, and individual features of your profile: Basic Information (which includes Gender, Birthday, Hometown, Political and Religious Views, and Relationship Status), Personal Information (which includes your Interests, Activities, Favorites and your About Me section), photos and videos tagged of you, status updates, online status, friends, wall, education and work information. On the Contact Information tab, you can tailor permissions for IM Screen Name, Mobile Phone, Land Phone, Current Address, Website and Email Address (if in fact you provided these details for your profile).

- To limit viewing of Profile information to only your Facebook friends, select "All Friends" in each drop-down menu. If you wish to limit viewing to certain segregated lists of friends that you can set up on your main Friends page, or just to individual friends, or to exclude certain individuals and networks, choose "Customize" in the drop-down menus and adjust the settings accordingly.

Search: You can control which Facebook users can find you in searches and what appears in your search listing within the site; more importantly, you can control whether you are searchable by anyone on public search engines. Within Facebook, you can restrict which networks have access to your profile in searches and what actions people can take with your search results, such as contacting you or adding you as a friend.

- To be searchable only by your Facebook friends, select "All Friends" in the Search Visibility drop-down menu and leave the first set of checkboxes below the drop-down menu blank.
- To avoid being searchable on public search engines, when you have selected "Everyone" in the drop-down menu simply uncheck the box next to "Create a public search listing for me."

News Feed and Mini-Feed: This page has three tabs. On the "Actions Within Facebook" tab, you can control what actions show up automatically in your Mini-Feed and your friends' News Feeds.

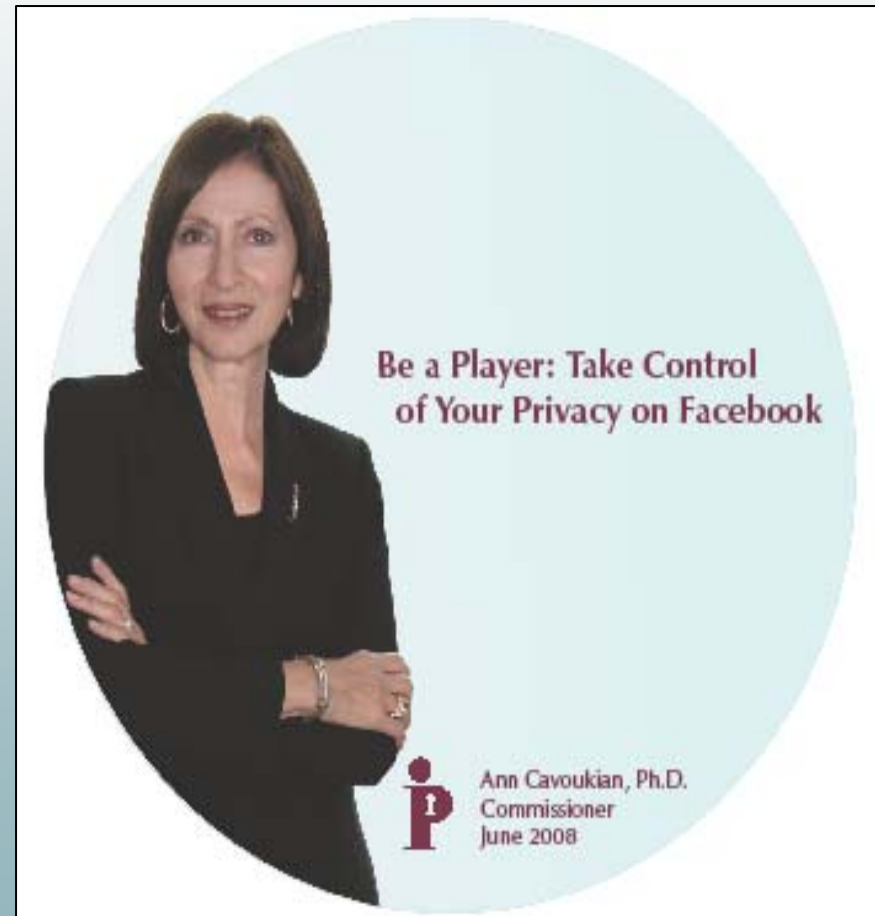
- "Uncheck" any actions that you do not want your friends to know about automatically, such as when you make a comment on a posted item or add a friend.

On the "Actions on External Websites" tab, you can opt out of having your activity on external websites of certain partner organizations posted to your Facebook profile's Mini-Feed, where it may also appear on your friends' News Feeds. This is a feature known as Facebook Beacon; there are numerous partner websites including Epicurious, Typepad, Blockbuster, etc.



Joint IPC-Facebook Video: *Be a Player: Take Control of Your Privacy on Facebook*

- Issues covered in our video include weak privacy controls, the intrinsic risks involved in using them, and some of the protections students should be aware of when posting their personal information online, such as being able to control access to one's profile and being able to block access to specific information.
- This video can be viewed at www.ipc.on.ca or for a free copy, please email our office at publicat@ipc.on.ca.





Conference on Youth Privacy

- Last year, the IPC held a conference *Youth Privacy Online: Take Control, Make It Your Choice!* – attended by professionals from a diverse range of public and private sector organizations including education, technology and social studies.
- The conference also highlighted the work of my office in developing and distributing educational materials to schools. To date, we have distributed:
 - **8,500** copies of our brochure – *When Online Gets Out of Line: Privacy - Make an Informed Online Choice*
 - **7,000** copies of our Tip Sheet – *How to Protect Your Privacy on Facebook*
 - **500** copies of our brochure – *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*
 - **500** copies of our DVD – *Be A Player: Take Control of Your Privacy on Facebook*
- We have also recently updated our IPC School-Kits to include material on how to safely navigate and engage in online social activities.



Youth Privacy Online:

Take **Control**

Make it **your choice!**



September 4, 2008  Eaton Centre Marriott  **Be there!**



IPC School Kits

- The IPC has been distributing school kits all across Ontario for more than a decade;
- These kits target Grades 5, 10, 11, and 12;
- The kits are designed to assist educators in teaching children about various topics including: privacy; personal information; open government; transparency; freedom of information laws; and how to access government information.
- As part of a major update, additional lessons about online social networking are being added to the teachers' kits.

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



A Study Guide for Secondary Schools
Grade 10 Teacher's Guide
May 2008



*SmartPrivacy
and
Privacy by Design*



SmartPrivacy

www.smartprivacy.ca



Privacy by Design – “The sine qua non”

LAW - REGULATION & INDEPENDENT OVERSIGHT

EDUCATION & AWARENESS

ACCOUNTABILITY & TRANSPARENCY

SOCIETAL NORMS

MARKET FORCES

Data Security

Fair Information Practices

“SmartPrivacy is the umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protections to education and awareness, but one measure stands out as the sine qua non: Privacy by Design. Dr. Ann Cavoukian, Information & Privacy Commissioner of Ontario, Canada, August 13, 2009.”



www.privacybydesign.ca



Privacy by Design: The 7 Foundational Principles

1. *Proactive* not Reactive;
Preventative not Remedial
2. Privacy as the *Default*
3. Privacy *Embedded* into Design
4. Full Functionality: Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy



Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept that I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we understand that a more substantial approach is required – extending the use of PETs to taking a positive-sum, not a zero-sum, approach.

Privacy by Design now extends to a "Triology" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy protection requirements tend to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

1. *Proactive* not Reactive; *Preventative* not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.



How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca