



***Social Networking and Privacy:
You must architect both into the
service you provide***

**Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario**

**International Symposium:
Privacy in the Age of Social Network Services
Strasbourg, France
October 13, 2008**



Presentation Outline

- 1. Privacy = Freedom*
- 2. Online Social Networks*
- 3. Facebook / MySpace*
- 4. Looking at Privacy Differently*
- 5. Conclusions*



Privacy = Freedom



Information Privacy Defined

Information Privacy: Data Protection

- Freedom of choice; personal control; informational self-determination;
- Control over the collection, use and disclosure of any recorded information about an identifiable individual;
- Privacy principles embodied in “Fair Information Practices.”



Online Social Networks



Online Social Networks

- A social network service builds online networks for communities of people who share interests and activities or who are interested in exploring the interests and activities of others;
- Most services are primarily web-based and provide a collection of various ways for users to interact, such as chat, messaging, email, video, voice chat, file sharing, blogging, discussion groups, etc.;
- The main types of social networking services are those which contain directories of some categories (such as former classmates), the means to connect with friends (usually with self-description pages), and recommender systems linked to trust.



Online Social Networks

Privacy Issues

- **Privacy notices**
- **Privacy settings**
- **Sharing of information**
- **Third-party applications**
- **Deleting your profile**
- **Cyber-bullying**
- **Identity theft**



Facebook



Joint Project with Facebook

- In 2006, I was approached by senior executives from Facebook seeking my input on their privacy measures;
- Facebook and my office developed a joint brochure for university students outlining privacy tips when using online social networking sites;
- But first, my office convened a Focus Group of university students to learn first-hand what they thought about online social networks.



IPC Student Focus Group

- On August 24, 2006, we held a Focus Group with 20 university students (from major universities in Canada) to discuss their views of online social networking;
- In particular, all of the students except one were active users of **Facebook** and strongly favoured it;
- The participants recounted real, practical stories about their personal experiences, indicating that they frequented the Facebook website multiple times each day.



Results of Our Student Focus Group

- Online social networking is an overwhelmingly popular experience for university students;
- However, most students were unaware of the privacy issues, or how their personal information could be used by various websites. No one had set their privacy filters (most being totally unaware of them); no one had even read the privacy policy.



Privacy Concerns Raised

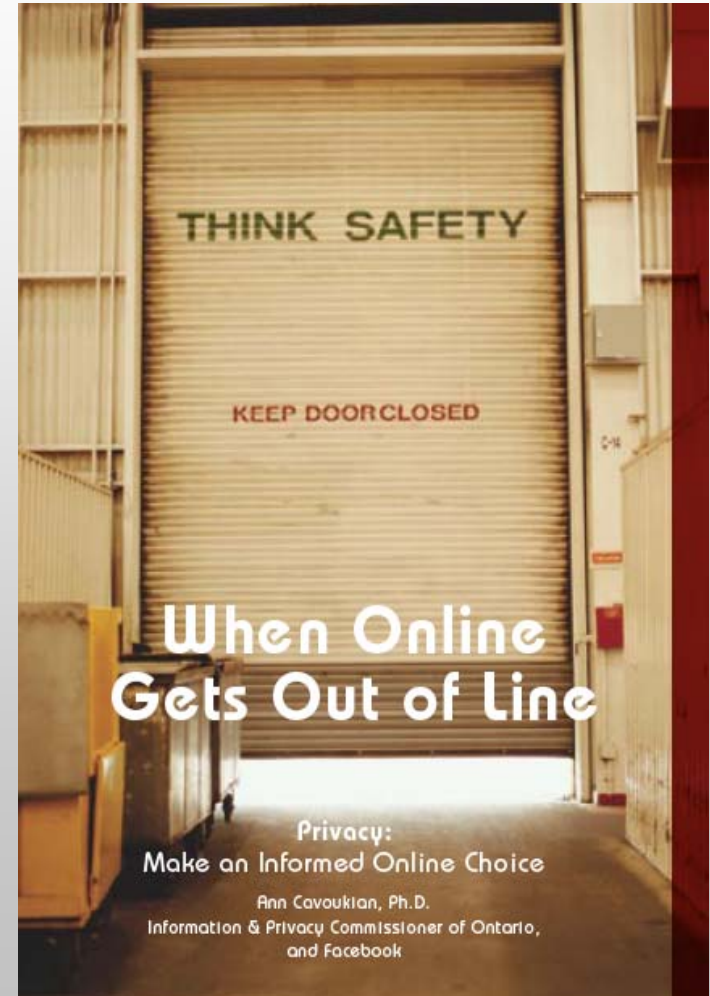
- People give out too much personal information about themselves online, believing that their information is “private” and they are safe behind the screen – they are not;
- This mistaken belief can lead to undesirable events, as a result of individuals being tracked through their social networking profiles:
 - Expulsion from universities and colleges due to nature of some information contained on their profiles;
 - Investigations by authorities due to information posted on profiles;
 - Being fired from employment due to information posted on profiles;
 - Misuse, selling or “databasing” of personal information;
 - Stalking and harassment;
 - Assault (physical).



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.






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
COUNSELLORS OF ONTARIO

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.

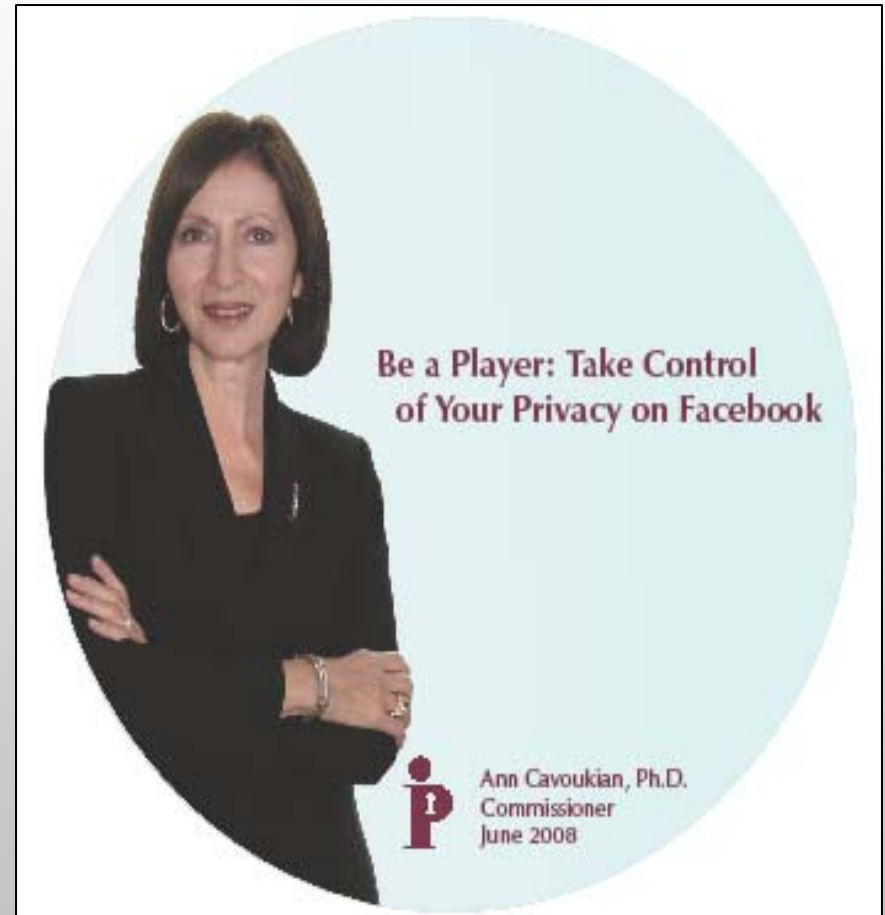
- "Uncheck" any actions that you do not want your friends to know about automatically, such as when you make a comment on a posted item or add a friend.

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.



IPC Facebook Privacy Video

- Issues covered in this 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.





My Advice to Students

Remember the 5 P's:

- **Predators**
- **Professors**
- **Prospective employers**
- **Parents**
- **Police**

*Nothing you post online is ever private,
and anything you post online can
remain there forever.*

IPC Event: Youth Privacy Online



Youth Privacy Online:

Take **Control**

Make it **your choice!**



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



MySpace

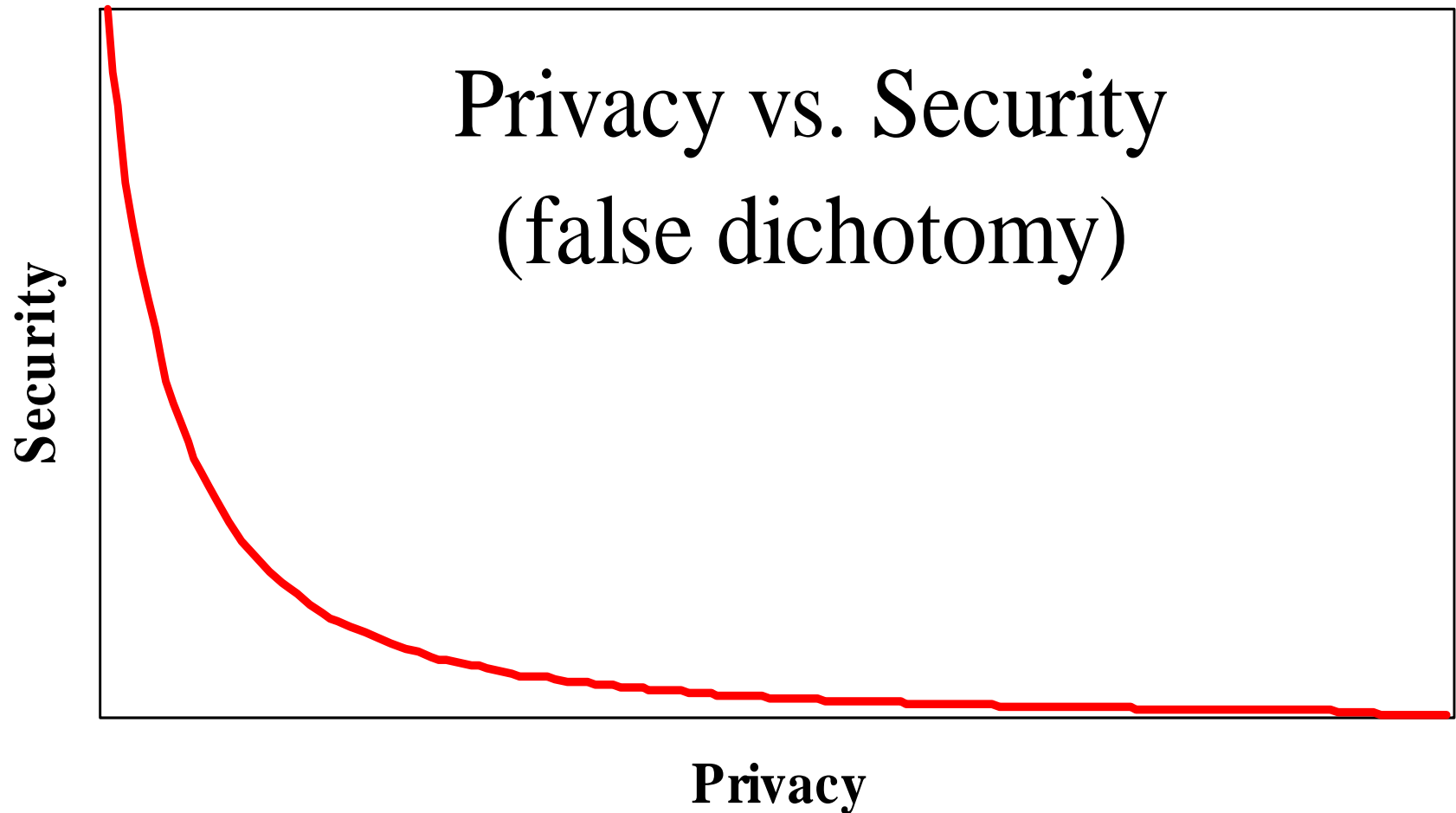
- In September, I met with senior executives from MySpace to discuss the privacy options available on their website as well as privacy-related educational tools and guides;
- We are currently working towards building a constructive relationship with MySpace and look forward to promoting privacy for MySpace users.



Looking at Privacy Differently



Privacy OR Security: *A Zero-Sum Game*





Positive-Sum
NOT
Zero-Sum



Positive-Sum Model

*Change the paradigm
from a zero-sum to
a positive-sum model:
Create a “win-win” scenario,
not an “either/or”
involving trade-offs*



Privacy by Design: “Build It In”

- Build in privacy – up front, into the design specifications into the architecture; if possible embed privacy right into the technology used – *bake it in*;
- Assess the risks to privacy: conduct a privacy impact assessment; follow up with annual privacy audits;
- Data minimization is key: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- Use privacy enhancing technologies (PETs): give your customers maximum control over their data.



*From PETs
to
Trans Tech*



Transformative Technologies

**Surveillance Technology + Positive-Sum Paradigm +
Privacy Enhancing Technology =
Transformative Technologies**

Common characteristics of Transformative Technologies:

- Help minimize unnecessary disclosure, collection, retention and use of personal data;
- Empower individuals to participate in the management of their personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in (personal) data governance structures;
- Help promote and facilitate widespread adoption of those technologies.



Conclusions

- We cannot lose sight of the fact that the functionality of online social networking sites is to “network” and share information;
- A positive-sum paradigm allows users of social networking sites to share their information with people they choose and have controls available to protect their privacy – privacy by design;
- **Privacy revolves around freedom of choice and personal control.**



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