Ontario's Privacy Regime, Sine Qua Non: *"Privacy by Design"*

Ken Anderson
Assistant Commissioner (Privacy)
Ontario

Data Guidance Webinar
September 3, 2009

Presentation Outline

1. **The IPC: Who We Are and What We Do**
2. **What Do the *Acts* Cover?**
3. **Public Education and Privacy Research**
4. ***Privacy by Design – The Way of the Future***
5. **A Word from Commissioner Cavoukian on *Privacy by Design***

The IPC: Who We Are and What We Do

Who We Are And What We Do

- The Information and Privacy Commissioner is appointed by the Ontario Legislative Assembly – and is independent of the government of the day;
- The Commissioner's mandate includes overseeing the access and privacy provisions of these *Acts*:
  - *Freedom of Information and Protection of Privacy Act* (FIPPA);
  - *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA); and
  - *Personal Health Information Protection Act* (PHIPA).

Commissioner's Mandate

The Commissioner responsible for:

- investigating privacy complaints;
- resolving appeals from refusals to provide access to information;
- ensuring that organizations comply with the access and privacy provisions of the *Acts;*
- educating the public about access and privacy issues;
- conducting research to promote understanding of privacy and access issues; and
- commenting on proposed government legislation and programs that may affect privacy or access.

Reappointed for a Third Term

On May 27, 2009, Dr. Ann Cavoukian was reappointed as Information and Privacy Commissioner for the province of Ontario for an unprecedented third term.

"We are in the midst of profound change. Technology – which has resulted in many challenges – can also be tapped for innovative privacy solutions. I will continue to emphasize the need to embed privacy directly into IT. I look forward to the challenge – I have so many new ideas that I wish to pursue."

Plans for the Commissioner's Third Term

Privacy by Design:

Focus on *Privacy by Design* which is a concept Commissioner Cavoukian first developed in the 90s, when she began her campaign to enlist the support of technology to protect privacy, rather than encroach upon it;

Electronic Health Records:

Working with all stakeholders in the health care field to help bring about and effective and privacy-protective electronic health records system;

Automatic Disclosure Programs:

Strongly urging both provincial and local governments to be very proactive in developing automatic disclosure programs, in which general records are routinely posted to government websites.

What Do the Acts Cover?

FIPPA and *MFIPPA*

- The two public sector *Acts*, ***FIPPA*** and ***MFIPPA***, provide the public with access and privacy rights in regard to government held information, in accordance with the following principles:
  - Information should be available to the public;
  - Exemptions to the right of access should be limited and specific;
  - Protect the privacy of individuals with respect to information about themselves held by the government;
  - Provide the public with a right of access to that information and a right to correct inaccurate information.

The Jury Vetting Investigation

- This case focused on whether the privacy rights of prospective jurors were breached when police conducted background checks on jurors – by accessing confidential police databases – on behalf of certain Crown Attorneys;
- Commissioner Cavoukian ordered an investigation into whether this practice was limited to specific courthouses, or whether it was more widespread – in addition to whether it violated the privacy rights of jurors guaranteed by *MFIPPA*;
- As part of the investigation, we sent a formal survey to all 55 Crown jurisdictions to determine the extent to which Crown Attorneys have received background information about potential jurors;
- All 55 Crown jurisdictions have now completed this survey, and we are in the process of analysing the results.

Ontario's *PHIPA*

- *PHIPA* came into effect on November 1, 2004, and governs "personal health information" (PHI) in the custody or control of "health information custodians" and "agents" of health information custodians;
- Under *PHIPA*, consent is required for the collection, use or disclosure of personal health information (PHI), subject to specific exceptions. This consent must:
  - be a consent of the individual;
  - be knowledgeable;
  - relate to the information;
  - not be obtained through deception or coercion.
- *PHIPA* also provides individuals with:
  - a right of access to all records of PHI about them in the custody or control of any health information custodian (with some exceptions);
  - a right to correct their records of PHI (again, with some exceptions).

Oversight and Enforcement of *PHIPA*

- The Commissioner may investigate where:
  - a complaint has been received; or
  - the Commissioner has reasonable grounds to believe that a person has contravened or is about to contravene the *Act*.
- The Commissioner has powers to enter and inspect premises that require access to PHI;
- Where a complaint of a privacy breach is found to be valid, the Commissioner may issue a variety of Orders to alleviate harm and prevent future violations of the *Act*.

Public Education and Privacy Research

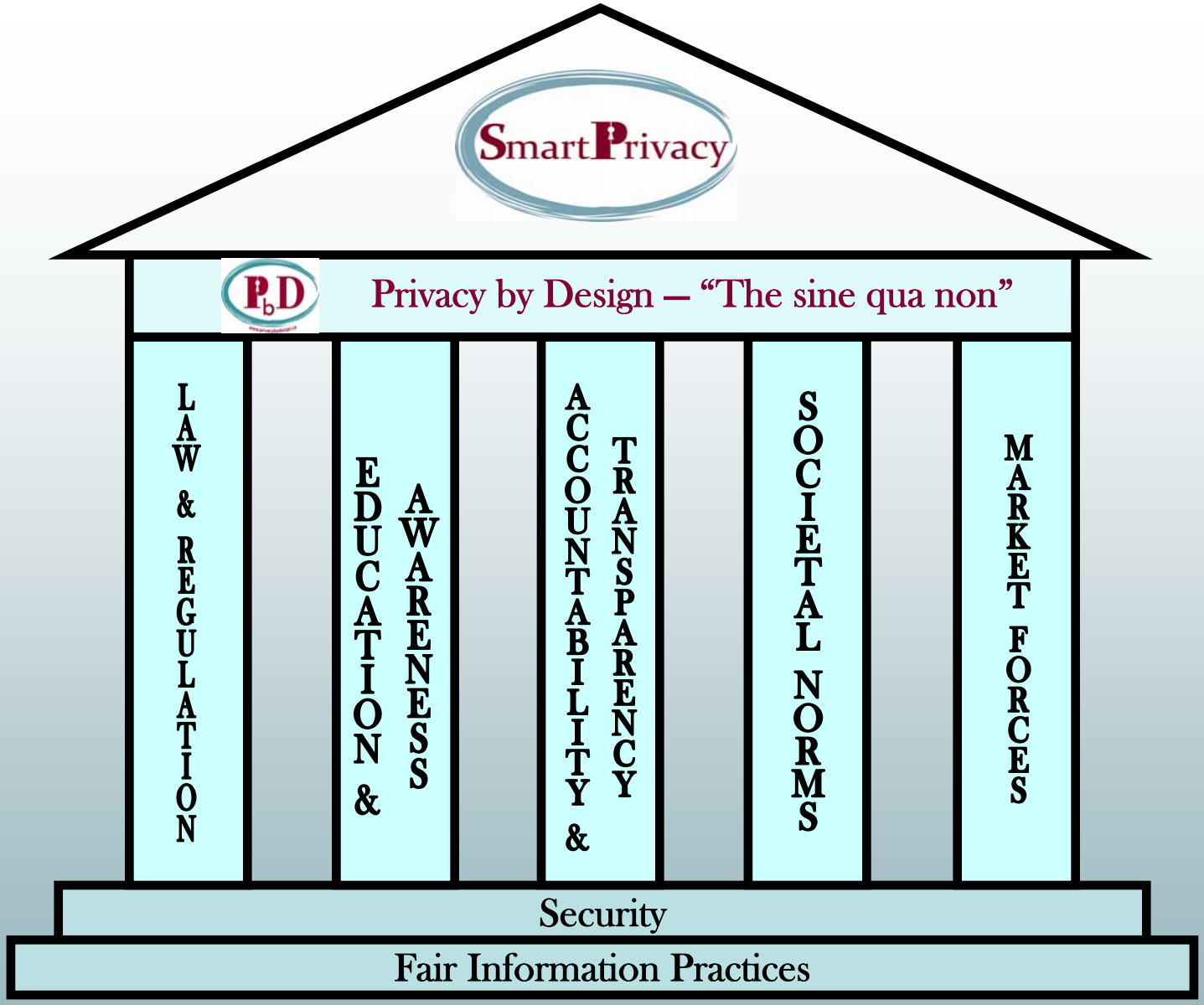
The Commissioner's Public Education and Privacy Research Role

- Apart from enforcement of the three *Acts*, the IPC has been active in promoting new ways of thinking about how best to protect privacy;
- Some of the public education and research initiatives of which we are particularly proud are:
  - Personal health records (PHR);
  - *Privacy by Design*;
  - Surveillance cameras
  - Enhanced driver's licences
  - Cloud computing; and
  - Social networking.

Personal Health Records

- The IPC is exploring PHI alternatives:
  - **Sunnybrook MyChart** – a patient portal that allows the patient to view their PHI stored in Sunnybrook Hospital's electronic records – this has been purchased by Telus, a Canadian telecom;
  - **Microsoft HealthVault** – Internet-based product that all allows patients to develop and control access to their own PHI (in Canada, Microsoft is working with Telus to deliver this service);
  - **Google Health** – Internet-based product that allows patients to enter their PHI or have their health care providers upload their PHI from compatible systems.
- The IPC recently published a toolkit alerting physicians to the privacy issues that must be considered in making the transition from paper-based to electronic records – *Personal Health Information: A Practical Tool for Physicians Transitioning from Paper-Based Records to Electronic Health Records* (available at www.ipc.on.ca).

Privacy by Design

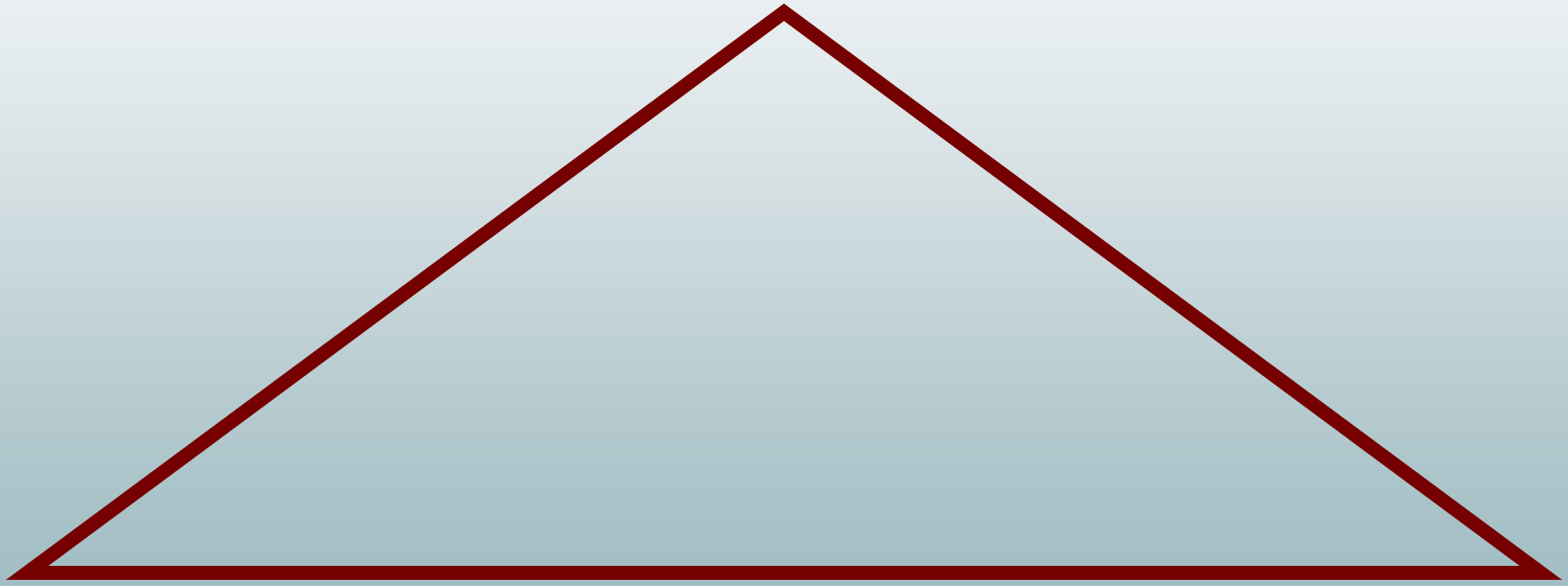


"SmartPrivacy is the umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protections to education and awareness, but one measure stands out as the sine qua non: *Privacy by Design. Dr. Ann Cavoukian, Information & Privacy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


PbD
www.privacybydesign.ca

Privacy by Design:
The Trilogy of Applications

Information Technology



Accountable Business Practices

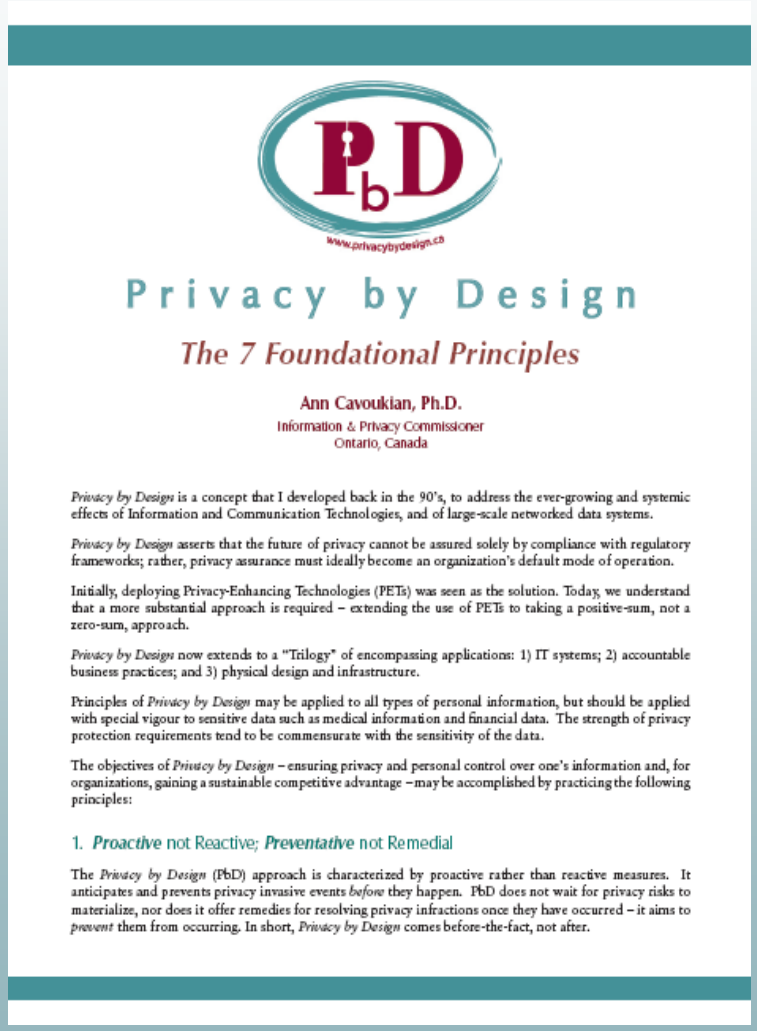
Physical Design & Infrastructure

Privacy by Design: *Focus for 2009*

- **Information Technology** – Building privacy directly into technology, at the earliest developmental stage;
- **Accountable Business Practices** – Incorporating privacy into competitive business strategies and operations;
- **Physical Design and Infrastructure** – Ensuring privacy in organizational and health care settings.

Privacy by Design:
7 Foundational Principles

1. *Proactive* not Reactive; *Preventative* not Remedial
2. Privacy as the *Default*
3. Privacy E*mbedded* 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



www.privacybydesign.ca

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 "Trilogy" 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:

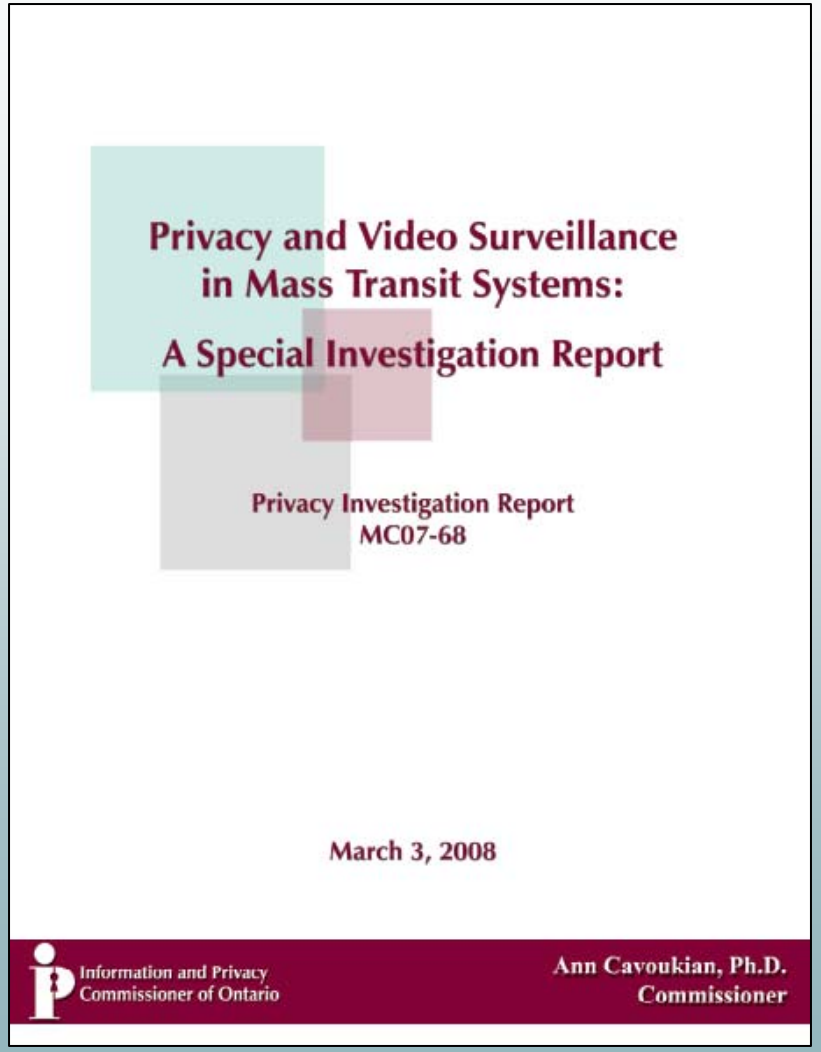
1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

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.

Available at **www.privacybydesign.ca**

TTC Surveillance Cameras

- In March 2008, we ruled that Toronto's Mass Transit System's use of video surveillance cameras was in compliance with Ontario's privacy law.
- However, we called upon the TTC to undertake a number of specific measures to enhance privacy:
  - Personal information will only be collected for legitimate, limited and specific purposes;
  - Collection will be limited to the minimum necessary and **only retained up to 72 hours;**
  - A comprehensive audit of the video surveillance system must be conducted by an independent third party using the GAPP (Generally Accepted Privacy Principles).



www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf

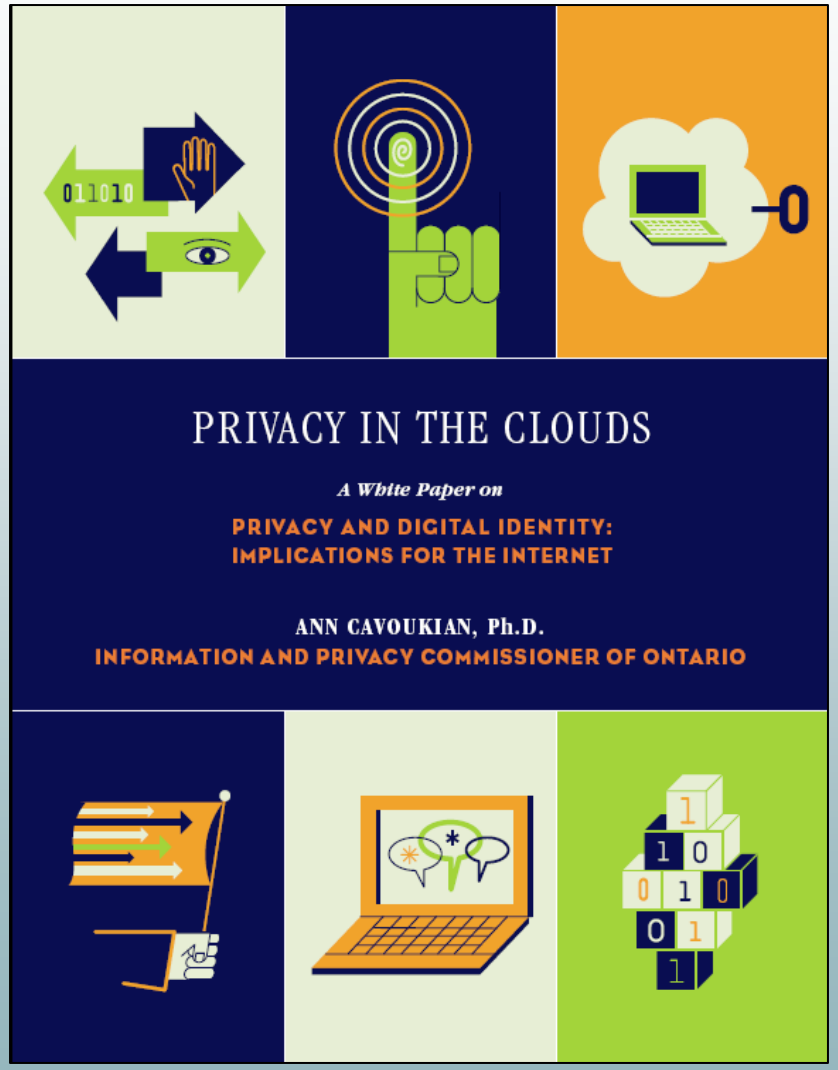
Enhanced Driver's Licences, RFIDs and "On-Off" Switches

- In 2008, the Ontario Government introduced legislation to authorize an enhanced driver's licence and photo card that incorporates a Radio Frequency Identification chip (or RFID) which transmits information that can be read from a distance by border officials;
- However, anyone with a readily available skimming device can also read the unique personal identifier number embedded in the RFID from a distance, raising concerns about possible identity theft, tracking and surveillance of cardholders;
- The Commissioner's response was a recommendation to the government to implement an "on-off" switch into the design of Ontario's new enhanced driver's licences.

Privacy in the Clouds

A White Paper on Privacy and Digital Identity: Implications for the Internet

- The 21st Century Privacy Challenge;
- Creating a User-Centric Identity Management Infrastructure;
- Technology Building Blocks;
- A Call to Action.



www.ipc.on.ca/images/Resources%5Cprivacyintheclouds.pdf

Cloud Computing

- Globally networked data systems, while purportedly benefiting the individual are often opaque and limit meaningful individual participation in the managing and controlling their personally-identifiable information (PII);
- Opaque data systems can diffuse accountability and inhibit responsibility for data loss or misuse;
- The emergence of the so-called energy 'Smart Grid' is case in point. Little is known about the personal data flows involved and how these may be safeguarded against hacking, unauthorized access, account takeovers, and fraudulent uses;

Cloud Computing (Cont'd)

- We seek effective management and control by both organizations and individuals over the entire data lifecycle, from collection, use, retention and disclosure. This can include, for example:
  - Improved transparency and openness;
  - Innovative and context-appropriate notices;
  - Meaningful user options;
  - Privacy by Design: privacy embedded into data systems early as the default;
  - Demonstrable and credible assurances/redress mechanisms.
- The name of the game is *trust*.

Smart Grid:
What is It?

- The smart grid refers to an electricity system that monitors and optimizes its interconnected elements (e.g., generators, high-voltage networks, energy storage installations, and end-use consumers including household appliances and devices);
- A smart meter is a meter that can record and report electricity consumption information automatically;
- In our jurisdiction of Ontario, old hydro meters which used to be read in person are being replaced by a smart meter.

SmartPrivacy for the Smart Grid:* *Privacy Risks*

- The information collected on a smart grid is a library of personal information, the mishandling of which could lead to the invasion of consumer privacy;
- An electricity usage profile could become a source of behavioural information;
- There will be major concerns if consumer-focused principles of transparency and control are not treated as essential design principles from start to end.

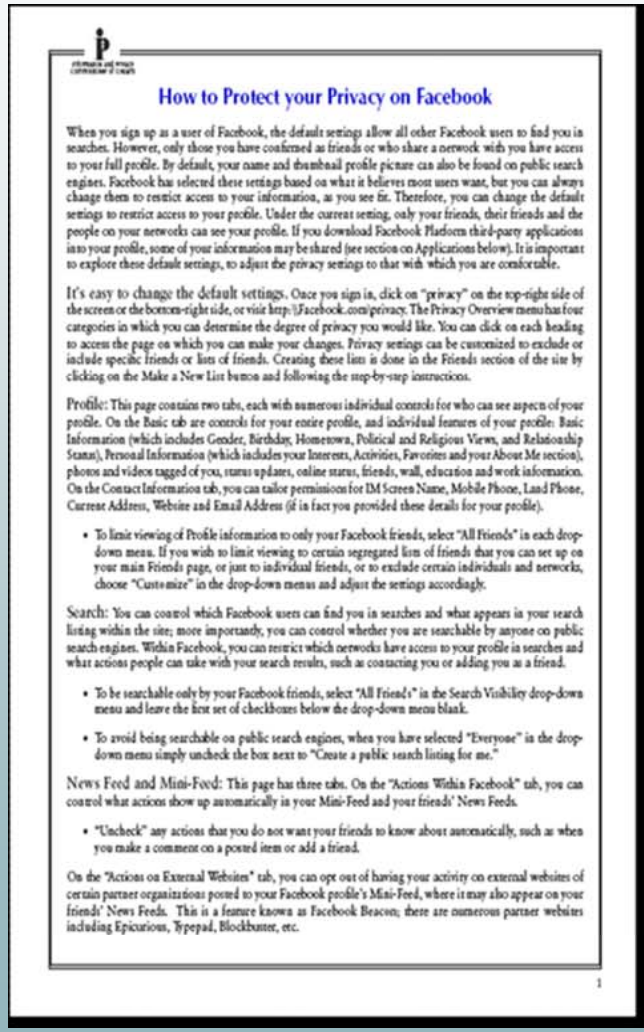
*SmartPrivacy

www.ipc.on.ca/english/About-Us/Whats-New/Whats-New-Summary/?id=113

Smart Grid:
Where the IPC stands

- The smart grid is a good idea, but the focus is so much on controlling energy use that the privacy issue is understated. We must take care not to sacrifice consumer privacy amidst an atmosphere of enthusiasm for the project of electricity reform;
- Principles of *Privacy by Design* must be part of the overall design for smart grid data flows;
- Fortunately, for the people of Ontario, the government consulted with the IPC, and made its 'smart metering entity' subject to our jurisdiction.

Social Networking Websites



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 permission 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.

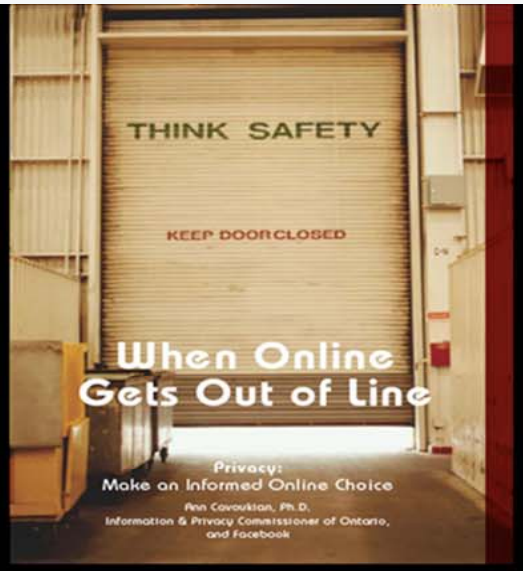
- To be searchable only by your Facebook friends, select "All Friends" in the Search Visibility drop-down menu and leave the first set of checkboxes below the drop-down menu blank.
- To avoid being searchable on public search engines, when you have selected "Everyone" in the drop-down menu simply uncheck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

1



A Word from Commissioner Cavoukian on *Privacy by Design*

Dr. Ann Cavoukian, Information & Privacy Commissioner of Ontario, Canada, describes her vision of the social benefits realized once organizations adopt her concept of *Privacy by Design*.

How to Contact Us

Ken Anderson

Assistant Commissioner (Privacy)/Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca