Digital Rights Management… and Privacy

Ken Anderson
Assistant Commissioner, Privacy

Office of the Information & Privacy Commissioner of Ontario
MITACS Workshop
June 23, 2010

Who We Are

Commissioner Ann Cavoukian, Ph.D.

- appointed by Ontario legislature
- independent from government
- oversees 3 privacy & access to information laws

Mandated to:

- investigate privacy complaints
- resolve appeals from refusals to provide access to information
- ensure organizations comply with access and privacy provisions of the *Acts*
- educate public about Ontario's access and privacy laws
- conduct research on access and privacy issues, provide advice and comment on proposed government legislation & programs.

Key Definitions

Information privacy refers to the right or ability of individuals to exercise control over the collection, use and disclosure by others of their personal information

Personally-identifiable information ("PII") can be biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, and is the stuff that makes up our modern identity

Required Privacy Protections

Any Digital Rights Management (“DRM”) scheme involving the collection, use or disclosure of personally identifiable information (“p.i.”) requires a strong privacy framework to protect p.i. based on “fair information practices”

Canada: CSA Code

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

The Ten Commandments

- Accountability
  - for personal information
  - designate an individual(s) accountable for compliance
- Identifying Purposes
  - purpose of collection must be clear at or before time of collection
- Consent
  - individual has to give consent to collection, use, disclosure of personal information

The Ten Commandments

- Limiting Collection
    - collect only information required for the identified purpose and information shall be collected by fair and lawful means
- Limiting Use, Disclosure, Retention
    - consent of individual required for other purposes
- Accuracy
    - keep as accurate and up-to-date as necessary for identified purpose
- Safeguards
    - protection and security required appropriate to the sensitivity of the information

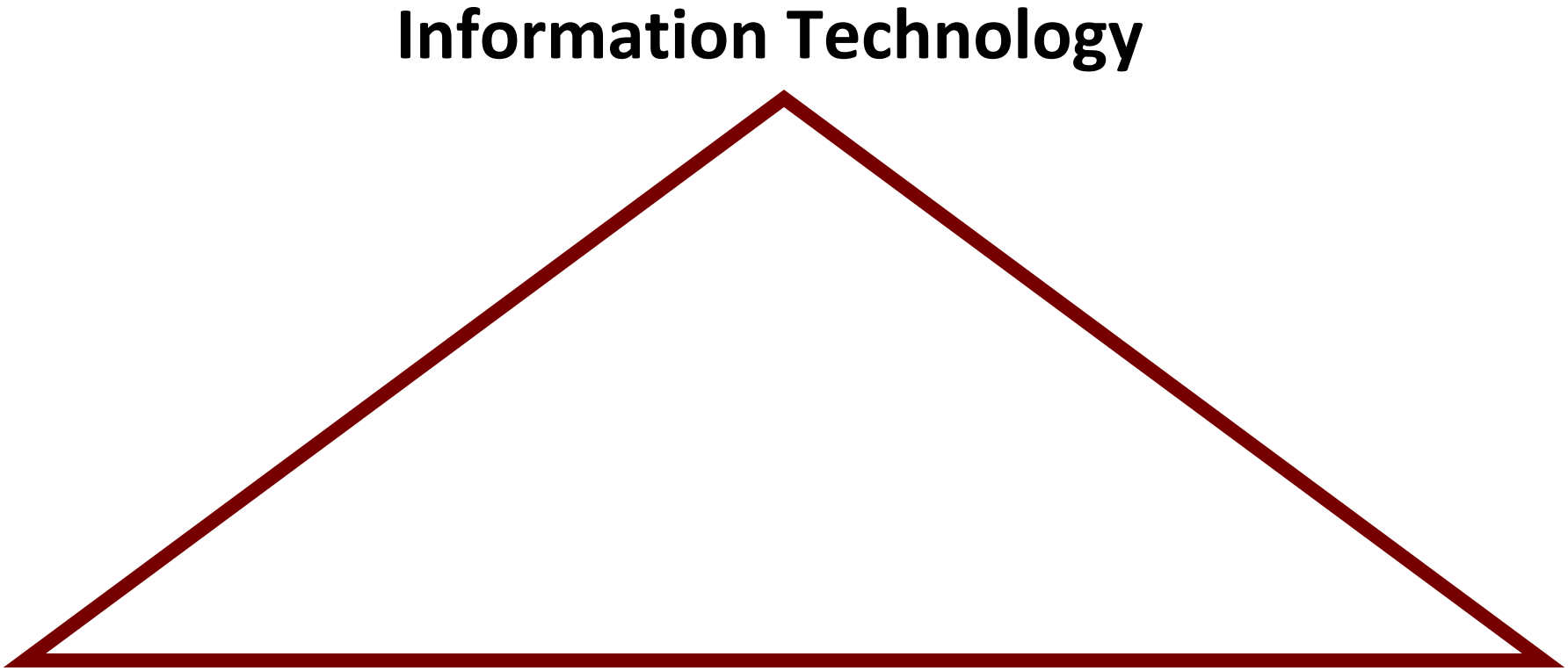
The Ten Commandments

- Openness
  - policies and information about the management of personal information should be readily available
- Individual Access
  - upon request, an individual shall be informed of the existence, use and disclosure of her personal information and be given access to that information, challenge its accuracy and completeness and have it amended as appropriate
- Challenging Compliance
  - ability to challenge all practices in accord with the above principles to the accountable body in the organization.

Privacy by Design: "Build It In"

- We first developed the concept of ***Privacy by Design*** in the 90s, as a response to the growing threats to online privacy that were beginning to emerge;
- ***Privacy by Design*** **seeks to build in privacy** – up front, right into the design specifications; into the architecture; embed privacy into the technology used – ***bake it in***;
- **Data minimization is key**: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- **Use PETs *Plus*** (positive-sum, not zero-sum) wherever possible: give people maximum control over their own data.

Privacy by Design:
The Trilogy of Applications



Privacy by Design:
The 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

PbD

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.

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

How to Contact Us

Office of the Information & Privacy Commissioner of 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**