Privacy by Design:
Integrating Technology into Global Privacy Practices

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario, Canada

Harvard Privacy Symposium

August 23, 2007

IPC

Role of the IPC

Role of the Information & Privacy Commissioner of Ontario (IPC) is set out in three statutes:

- *Freedom of Information and Protection of Privacy Act* (FIPPA);
- *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA);
- *Personal Health Information Protection Act* (PHIPA).

Mandate of the IPC

Under its statutory mandate, the IPC is 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 Ontario's access and privacy laws; and
- conducting research on access and privacy issues, and providing advice and comment on proposed government legislation and programs.

Privacy by Design

"Technology knows no borders …
technology transcends jurisdiction."

- This has been the driving force behind my office's approach to privacy, in shaping public policy and organizational practices, on a wide range of technology-related issues, including:
- RFIDs, biometrics, smartcards, PKI, DRM, P3P, identity management systems, video surveillance, national ID cards, electronic road toll systems, and Social Networks (Facebook).

IPC

“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 into the specs***;
- 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.

IPC

Privacy-Enhancing Technologies *(PETs)*

- The IPC developed the concept and methodology recognized around the world today as ***privacy-enhancing technologies*** (PETs);
- In 1995, the IPC and the Dutch Data Protection Authority published the landmark study, ***Privacy-Enhancing Technologies: The Path to Anonymity (Vols. I & II).*** www.ipc.on.ca/images/Resources/anoni-v2.pdf

Privacy Enhancing Technologies *(PETs)*

- Privacy Enhancing Technologies include those that empower individuals to manage their own identities in a privacy enhancing manner.

- These include tools or systems to:
  - anonymize and pseudonymize identities;
  - securely manage login IDs and passwords and other authentication requirements;
  - restrict traceability and limit surveillance;
  - allow users to selectively disclose their PII to others and exert maximum control over their PII once disclosed.

Recent IPC Publications on Privacy, Security and Technology

Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy

- Developed with chief scientist, Alex Stoinov, Ph.D., this paper discusses the merits of the biometric encryption approach to verifying identity, ensuring strong security, and protecting privacy;

  www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

RFID Privacy Guidelines

- Developed with EPCglobal Canada, this publication is the strongest, most complete set of RFID guidelines developed to date, and promotes compliance with Canadian federal and provincial privacy laws;

  www.ipc.on.ca/docs/rfidgdlines.pdf

Identity Theft Revisited: Security is Not Enough

- This publication outlines how any organization can protect itself and, most importantly, protect its customers.

  www.ipc.on.ca/userfiles/page_attachments/idtheft-revisit.pdf

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).

Mandate of the Legislation

- Requires consent for the collection, use and disclosure of PHI, with necessary but limited exceptions;
- Requires that health information custodians treat all PHI as confidential and keep it secure;
- Codifies an individual's right to access and request correction of his/her own PHI;
- Gives a patient the right to instruct health information custodians not to share any part of his/her PHI with other health care providers;
- Establishes clear rules for the use and disclosure of personal health information for secondary purposes including fundraising, marketing and research;
- Ensures accountability by granting an individual the right to complain to the IPC about the practices of a health information custodian; and
- Establishes remedies for breaches of the legislation.

PHIPA Order No. 5
Wireless Technology Results in Order

- ***PHIPA* Order No. 5** resulted from a methadone clinic that installed a wireless video surveillance system in its washroom to monitor patients providing urine samples;
- Video images were intercepted by a wireless rear view backup camera in a car outside of the clinic;
- The Clinic was ordered to strongly encrypt all wireless signals if wireless video technology was to be utilized, and to review encryption practices on an annual basis;
- The standard of practice created by this Order was that if healthcare providers choose to use wireless technology, then they must encrypt – strongly.

PHIPA Order No. 4
Stolen Laptop Results in Order

- Despite the known high risks of loss or theft, personal health information was transported out of a hospital on a portable device (a laptop) by a physician, without safeguards;
- The Hospital was ordered to either de-identify or encrypt all personal health information before allowing it to be removed from the workplace;
- ***PHIPA* Order No. 4** created the standard of practice expected regarding the removal of identifiable health information from a healthcare facility – if it's not encrypted, it's not in compliance with *PHIPA*.

Global Privacy Standard

- In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners convened for the sole purpose of creating a single Global Privacy Standard (GPS);
- Globalization and converging business practices created the need to harmonize various sets of fair information practices so that businesses and technology companies could turn to a single instrument for assessing whether their practices were privacy-enhancing;
- The GPS builds upon the strengths of existing codes, containing time-honored privacy principles, but reflects an enhancement by explicitly recognizing the concept of “data minimization” under the “collection limitation” principle;
- The final version of the GPS was formally tabled and accepted by Commissioners in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

www.ipc.on.ca/images/Resources/up-gps.pdf

Conclusion

- Recognizing that the laws of various jurisdictions must be respected, a single privacy standard, as reflected in the Global Privacy Standard, can serve as a useful benchmark for businesses and technology/software companies;
- Turning to technology to enhance privacy not only makes good privacy sense, regardless of jurisdiction, it also makes good **business** sense, offering a competitive advantage;
- Integrating technology into sound privacy practices will be an essential way forward to compliment the global framework of laws and policies in place.

IPC

How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/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

IPC