# Automatic Digital Identity Privacy and Trust

**Ann Cavoukian, Ph.D.**

**Information and Privacy Commissioner**

**Ontario**

**RFID Solutions Conference, Toronto**

***October 5, 2006***

IPC

# IPC: Our Role

The role of the Information and Privacy Commissioner/Ontario (IPC) is set out in three statutes:

- *Freedom of Information and Protection of Privacy Act*;
- *Municipal Freedom of Information and Protection of Privacy Act;*
- *Personal Health Information Protection Act* (the *Acts*).

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.

IPC

# A Few of Our Accomplishments

- Co-invented the concept and methodology recognized around the world today as *privacy-enhancing technologies* (PETs);
- Played a pivotal role in shaping public policy on a wide range of technology and privacy issues, including RFID, biometrics, smartcards, PKI, Digital rights management technologies (DRM), P3P, identity management systems, video surveillance, customer relationship marketing, and electronic road toll system;
- Establishing and promoting internationally-accepted principles for developing privacy-enabled universal identity and authentication systems, through Microsoft and the broader open-source community;
- Setting international standards for privacy-protective development and deployment of biometric technologies through her membership on the Board of the International Biometrics Advisory Council (IBAC);
- Continuing to press for stronger security methods and techniques on the part of organizations to combat the current epidemic of spyware, phishing, pharming, and identity theft.

IPC

# How We Connected with EPCglobal Canada

Both the IPC and EPCglobal Canada believed there was a need to address the public's concern about privacy – ***in a proactive manner***.

IPC

# IPC Philosophy
## *Encapsulated in the 3C's:*

**Consultation**

- Opening the lines of communication;

**Collaboration**

- Working together to find solutions;

**Co-operation**

- No confrontation in resolving privacy issues.

IPC

# IPC Partnerships

- **Canadian Marketing Association** – "Incorporating Privacy into Marketing and CRM;"
- **Deloitte & Touche** – "The Security-Privacy Paradox: Strategies to address Privacy Issues and Misconceptions;"
- **PriceWaterhouseCoopers/Guardent** – Jointly developed the "Privacy Diagnostic Tool."

IPC

# Privacy Fundamentalists

- Feel that they have lost much of their privacy and are strongly resistant to any further erosion;
- For them, the right to privacy is absolute;
- No concept of balancing privacy with other interests no matter how important the other interests may be;
- Often the loudest and strongest voices heard on privacy issues – ***very appealing to the media.***

IPC

# Taking a Pragmatic Approach

- The brand of privacy I practice as a Privacy Commissioner is ***"practical privacy"*** — it has to work, on the ground;
- Try to take a balanced approach, resulting in a win-win scenario, whenever possible;
- Caution that ignoring privacy problems in the short-term, will only create bigger problems in the long-term.

IPC

# One of Many Benefits of RFIDs
## *Healthcare / Pharma*

- Tracking the authenticity, tracing the pedigree of pharmaceutical products;
- Tracking and inventory of patient specimens (blood samples, vials, test tubes, etc.);
- Tracking and inventory of hospital equipment.

IPC

# IPC DVD

## *A Word About RFIDs and your Privacy… in the Retail Sector*

- Spring 2006: my office released a short video clip discussing RFID tags and privacy;
- The IPC strongly supports the use of RFID technologies throughout the supply chain;
- Caution advised whenever linking item-level RFID tag data to individuals: ***privacy concerns raised***;
- We support technological solutions that can help mitigate consumer privacy concerns and trust issues.

**Watch online:** **www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=17035&U_ID=0**
**Order a copy:** **ipc.publication@ipc.on.ca**

# The Bottom Line

Privacy should be viewed as a **business** issue, not a ***compliance*** issue

IPC

# Law and Regulation

**Heightened Public Interest / Legislative Activity:**

- U.S. state bills, laws;
- Canadian & European privacy laws;
- Enhanced regulatory scrutiny, e.g..:
  - U.S. Congress RFID Caucus;
  - EU RFID consultations.

IPC

# Examples of U.S. RFID Laws

**Examples of state bills that have been passed:**

- **California AB1489** – requires certain point-of-sale devices to be equipped with a "tactually discernible numerical keypad" or other technology (such as a RFID device), in order to provide visually impaired persons "… the same degree of privacy … available to all individuals;"

- **New Hampshire HB1738** – prohibits the state use of surveillance devices (including a RFID device) on highways to identify motor vehicles, unless authorized by statute or in certain other circumstances;

- **Wisconsin AB290** – Prohibits requiring an individual to undergo the implanting of a microchip.

IPC

# Trends - U.S. Bills relating to RFID

## *introduced in 2006*

- Bills may be advancing through the legislative process, or they may be vetoed, stalled or have died;
- **Task Forces –** Bills that would establish task forces to study RFID technology in the public and/or private sector e.g.: New York, Washington;
- **Consumer Privacy –** Bills that would require notification of consumers of RFID tags and/or removal of tags at point of sale; e.g.: Illinois, Missouri, New York, Tennessee;
- **Prescription Drug Packaging –** Bills that would require packaging to incorporate RFID tagging technology (or similar trace and track technologies), among other things; e.g.: Federal bills

IPC

# Trends - U.S. Bills relating to RFID *introduced in 2006 (cont'd)*

**Human Identification:**

- ***Microchips in Individuals*** – Bills that would prohibit requiring microchips in individuals, e.g.: New Jersey, Ohio;
- ***Identification Documents*** – Bills that would restrict or prohibit the broadcasting or remote scanning of personal information on government ID documents via "contactless integrated circuits" or "radio waves," e.g.: Alabama, Illinois, Washington;
- ***Other Tracking*** – Bills that would restrict the use of RFID devices by state or municipal agencies for the purpose of tracking the movement or identity of individuals as a condition of obtaining a benefit or services, e.g.: Rhode Island.

IPC

# Risks of Not Addressing Privacy Concerns

A lack of attention to privacy can result in a number of negative consequences:

- harm to customers whose personal information is used or disclosed inappropriately;
- damage to your organization's reputation and brand;
- financial losses associated with deterioration in the quality and integrity of personal information;
- financial losses due to a loss of business or delay in the implementation of a new product or service due to privacy concerns;
- loss of market share or a drop in stock prices following negative publicity about a "privacy hit;"
- diminution of confidence and trust in the industry;
- violations of privacy laws.

- **IPC Publication:** *Privacy and Boards of Directors: What You Don't Know Can Hurt You*, www.ipc.on.ca/docs/director.pdf

IPC

# Privacy and RFID Tags

- RFID tags contain information about a product, not an individual (e.g., EPC, size, colour, manufacture date, etc.);
- Fueled by privacy fundamentalists, many consumers perceive a threat to privacy from RFID tags;

— **Consumer Reports** magazine, June, 2006 cover story:

***"The End of Privacy?***

***Tiny devices attached to everything you buy could put you under extensive surveillance."***

IPC

# Common Misconceptions

**Messaging Advanced – RFID tags will facilitate:**

- Unauthorized and surreptitious collection of personal information from RFID-tagged items;
- The linking and merger of product information and personal information, without consent;
- The ability to track consumers who have purchased various products, expanding the creation of personal profiles;
- The establishment of a widespread surveillance infrastructure.

IPC

# Absence of Privacy

- A failure to build privacy into the design and implementation of RFID-enabled information systems may produce a strong consumer backlash;
- This can have an adverse impact on a company's reputation, and ultimately, affect their bottom line;
- Case Examples:
    - Benetton
    - Metro AG
    - Gillette

IPC

# CASPIAN Boycott

## *Consumers Against Supermarket Privacy Invasion and Numbering*

- August, 2003: CASPIAN launched a worldwide boycott of Gillette products;

  "RFID tags in Gillette product packaging have been used with hidden shelf cameras to snap photos of unsuspecting customers. Since Gillette has not responded adequately or truthfully to consumer concerns, we are advising consumers to avoid all Gillette products, including shaving items, Duracell batteries, Braun appliances, and Oral B products until further notice."

  www.nocards.org/protest/index.shtml

IPC

# Metro AG

- In 2004, German supermarket Metro AG, the country's largest retailer and fifth-largest in the world, unveiled its “future store” to the public — a showcase of RFID technology;
- In introducing the technology, the store assured the public that whenever RFID technology was used it would make it visible and that the chips would never be used to store customer data;
- Those claims, as uncovered by K. Albrecht during her tour of the store, turned out to be false.

IPC

# Metro AG (Cont'd)

**What NOT to do: Covert Tracking:**

- Without notifying customers, Metro AG hid RFID tags in customer-loyalty cards, linking purchases with customer identity;
- Metro AG also embedded RFID in shopping carts to track customer movements in the store without notifying them;
- A public relations disaster ensued.

IPC

# Questionable Approach

- Do not acknowledge that privacy may be a potential problem; act like it doesn't exist;

***"What consumers don't know, won't hurt them."***

IPC

# Progressive Approach

- Ignoring the problem rarely works;
- Hiding the problem becomes the story;
- In the long run, trying to evade this issue is a poor business strategy;
- Be proactive and address the privacy issue head on.

IPC

# Benefits and Concerns

- **Get ahead of the story:** immunize consumers against the extreme messaging advanced by privacy fundamentalists;
- Companies need to emphasize the benefits of RFID, while at the same time, also addressing consumers' privacy concerns;
- So, how to respond? …

IPC

# Follow Privacy Principles

- Widespread agreement that a fair information practices approach to RFID technology is the right approach;
- Widespread agreement that early standardization and guidance is preferable, before the technology has been widely adopted;
  - Give notice;
  - Obtain consent;
  - Be open and transparent;
  - Allow user control;
  - Respect use limitation.

IPC

# Canada's Fair Information Practices

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

***CSA Model Code for the Protection of Personal Information***
(Privacy Code) CAN-CSA Q830 1996
www.csa.ca/standards/privacy/code/

IPC

# Canada's Fair Information Practices

- CSA Model Privacy Code was incorporated into Canada's federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) – appended as a schedule;

  www.privcom.gc.ca/legislation/02_06_01_01_e.asp

- Organizations that comply with the Privacy Code can be confident that they meet the federal requirements;

- In 2001, the European Commission recognized PIPEDA provides adequate protection for personal data transferred from the EU to Canada.

IPC

# Canada's Federal Private Sector Privacy Law: *PIPEDA*

As of 2004, the federal *Personal Information Protection and Electronic Documents Act* applies to:

- All personal information collected, used or disclosed in the course of commercial activities by provincially or federally regulated organizations;
- Unless a substantially similar provincial privacy law is in force.

IPC

# Provincial Private-Sector Privacy Laws

**Québec**: *Act respecting the protection of personal information in the private sector;*

**B.C.**: *Personal Information Protection Act;*

**Alberta**: *Personal Information Protection Act;*

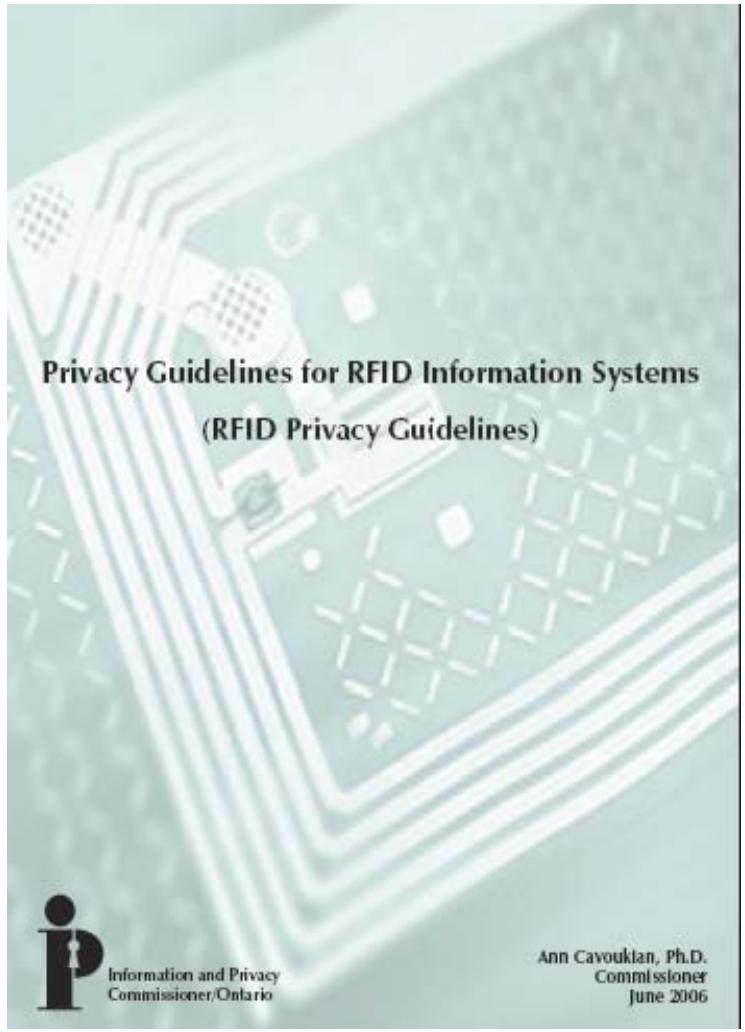
**Ontario:** *Personal Health Information Protection Act.*

IPC

# IPC RFID Privacy Guidelines

- Developed with leading industry standards-setting organization (GS1/EPCglobal Canada);
- Promotes compliance with Canadian federal and provincial privacy laws;
- Strongest, most complete set of RFID guidelines developed to date – promotes compliance and consumer trust around the world.

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




IPC

# Features of IPC RFID Guidelines

- The *Guidelines* address key privacy issues regarding use of item-level RFID technology in the retail/commercial sector;
- Goal: to promote RFID technology by addressing concerns about the potential threat to privacy and to build-in the necessary protections for the item-level use of RFID tags by retailers;

**The *Guidelines* are based on three principles:**

1. Focus on RFID information systems, not technologies;
2. Build in privacy and security from the outset, at the design stage;
3. Maximize individual participation and consent.

IPC

# Why We Collaborated with EPCglobal Canada

- To encourage the development of new technologies that allow for de-activation, preferably followed by re-activation;
- Encourage the concept of privacy by design:

  *"Embed privacy protective measures into the actual design and infrastructure of any new technology, including RFIDs."*

IPC

# Why You Need to Be Prepared

- Checkpoint Systems Inc. announced in September, 2004, that it had developed new RFID solutions for tracking individual consumer items;
- CASPIAN claimed that:
  - Checkpoint was developing RFID "spychips" for three well-known clothing labels;
  - Consumers wearing the tagged clothing could potentially be identified and tracked by readers;
- CASPIAN warned: ***"[We] will be working with consumers on an aggressive response to this privacy threat. Roll up your sleeves and get ready for a good fight."***

IPC

# Conclusion

- Strong need to address the public's concerns about privacy, in a proactive manner;
- Strong need to balance privacy with other interests - ***Practical Privacy****;*
- Ignoring privacy problems in the short-term, will only create bigger problems in the long-term;
- Build privacy into the design and implementation of RFID tags – ***"Privacy by Design;"***
- Immunize consumers against the extreme messaging advanced by some privacy fundamentalists;
- Emphasize the benefits of RFIDs while at the same time, also addressing consumers' privacy concerns;
- Follow universally accepted privacy principles;
- Be prepared for a ***"good fight."***

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