Privacy and Security:
How Technology Can Advance Both

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

State of Arizona

Office of the Auditor General

March 2, 2006

Information Privacy Defined

- **Information Privacy: Data Protection**
  - Freedom of choice; personal control; informational self-determination;
  - Personal control over the collection, use and disclosure of any recorded information about an identifiable individual.

Security ≠ Privacy

Privacy and Security: *The Difference*

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation

Security:

Organizational control of information through information systems

- Privacy; Data Protection
- Fair Information Practices

Understanding the Difference: *Privacy and Security*

- While security and privacy share some important common qualities and features, **security is *not* privacy;**
- Privacy means the protection of the *individual;*
- Security tends to look at information management practices from a top-down control perspective in an effort to protect company data, processes and systems from attackers;
- IT security professionals often make the mistake of believing that if data can be kept confidential and preserved from corruption, then privacy is guaranteed.

Fair Information Practices: *A Brief History*

- OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980);
- EU *Directive on Data Protection* (1995);
- Canada *Personal Information Protection and Electronic Documents Act* (PIPEDA) (2000);
- U.S. *Safe Harbor Framework Agreement* (2000).

United States
Safe Harbor

Safe Harbor Privacy Principles:

1. Notice
2. Choice
3. Onward Transfer
4. Security
5. Data Integrity
6. Access
7. Enforcement

As of March 1 2006, there were 870 businesses signed under the Safe Harbor Agreement.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Eight Principles:

1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

Privacy Laws Around the World

Uruguay: *Data Protection Act* (2004);
Tunisia: *Data Protection Act* (2004);
Japan: *Protection of Personal Information Act* (2003);
Sri Lanka: *Information and Communication Technology Act* (2003);
Bulgaria: *Personal Data Protection Act* (2002);
Canada: *Privacy Act (1982); Personal Information Protection and Electronic Documents Act* (2000);
Argentina: *Personal Data Protection Act;*
India: *Information Technology Act* (2000);*

Chile: *Data Protection Act* (1999);
United Kingdom: *Data Protection Act* (1998);
Hong Kong: *Personal Data Ordinance* (1996);
European Union: *Data Protection Directive* (1995);**
Taiwan: *Computer-Processed Personal Data Protection Law* (1995);
South Korea: *Protection of Personal Information Act* (1994);
Israel: *Protection of Privacy Law* (1992);
Australia: *Federal Privacy Act* (1988);***

* There is no general data protection law in India. The Information Technology Act is a set of laws intended to provide a comprehensive regulatory environment for electronic commerce addressing computer crime, hacking, damage to computer source code, breach of confidentiality and viewing of pornography.

** Member states of the EU have their own national privacy laws but are still required to meet the EU threshold.

*** In 2000, the Australian government passed an amendment to the 1988 Federal Privacy Act known as the Privacy Amendment (Private Sector) Act 2000.

United States

*Sectoral Laws: A Sample**

- 2005: North Carolina SB1048 “ID Theft Protection Act”
- 2005: FTC “Disposal Rule”
- 2003: California SB1386
- 2002: Sarbanes-Oxley
- 2000: Children's Online Privacy Protection Act
- 1999: Gramm-Leach-Bliley

* *This List represents only a small sample of sectoral laws in the United States.*

Current Privacy Notices:
A Waste of Paper?

- Annual privacy notices required by the Gramm-Leach-Bliley Act of 1999 are too complicated for most consumers to understand;

  "Each year banks and other financial institutions bear the cost of mailing mandatory notices to their many millions of customers, even though we suspect that most of the notices go from postman to trash can without ever being read."

  — John Dugan, Comptroller of the Currency, February 2006.

- **The fault for the complexity of the notices lies with regulators who created a model standard for banks in 2000 that was too technical;**

- Further, lawmakers also need to create a single national standard for data security; *"State laws differ from each other, sometimes subtly, sometimes significantly, from the circumstances that trigger a breach notice to consumers to the acceptable delivery mechanism for the notice."*

  — John Dugan, Comptroller of the Currency, February 2006.

Trend to Short Notices

- Short notices to the public came to be realized as a necessity when legislation governing privacy began to increase, prompting many organizations to accommodate as much of the new regulations as possible into their privacy statements and notices;

"When GLBA and HIPAA were passed, there was a requirement to make these notices even more complete and long. That has resulted in privacy notices that are barely readable and largely ineffective."

— Martin Abrams, Executive Director,
Center for Information and Policy Leadership,
Hunton & Williams LLP, 2004

Short Notices
International Efforts

- 2003, the movement to establish a global short privacy notice was officially recognized at the International Conference of Data Protection Commissioners in Sydney, Australia

- 2004, in Berlin, a working group of Commissioners (including the IPC), business leaders, lawyers and privacy practitioners met and prepared a memorandum recognizing that a new architecture was needed for privacy notices

- 2004, the EU Article 29 Working Group issued the position paper *WP100* on the use of "multi-layered notices"

Berlin Memorandum

- Effective privacy notices should be delivered within a ***framework*** with the following core concepts:

- **Multi-layered –** Privacy information should not be conveyed solely in a single document
- **Comprehension and Plain Language –** All layers should use language that is easy to understand
- **Compliance –** The total notices framework (all the layers taken together) should be compliant with relevant law
- **Format and Consistency –** Consistent format and layout will facilitate comprehension and comparison
- **Brevity –** The length of a privacy notice makes a difference *(maximum of seven categories)*
- **Public Sector –** These concepts have equal applicability to government collection and use of personal information

Why Short Notices are Important

Short notices:

- ensure that people are well informed about what an organization does with their personal information; and
- allow people to become empowered with a choice over their personal information.

The Short Notice

- ***Cleary, what is needed are more effective communications tools:***

- The short notice is an initial notice that an individual receives when personal information is first sought;
- The goal of the short notice is to provide all individuals with essential information in an easily readable and comparable format.

- **A short notice should include:**
  - who the privacy notice covers;
  - the types of information collected directly from the individual and indirectly from others about the individual;
  - uses or purposes for the data collected;
  - the types of entities that may receive the information (if it is shared);
  - information on choices available to the individual to limit use and exercise any access or other rights, and how to exercise those rights;
  - how to contact the organization for more information or to file a complaint.

Benefit of Short Notices

While individuals are the main beneficiaries of improved communication of information about an organization's privacy practices, there are also benefits for organizations:

- To communicate more effectively with the public, allowing for the growth of a relationship based on trust ***through simple understanding;***
- A standardized format could be used globally by an organization to provide for economies of scale.

Short Notices Under PHIPA

Role of the IPC

- In Ontario, the IPC has taken a leadership role in promoting the use of short notices in the health sector;
- Being the oversight body for PHIPA, the IPC has indicated that the notices prepared by health professionals must provide useful and understandable information to patients;
- The IPC wanted to ensure that patients are well informed of their rights and have the knowledge to exercise those rights;
- Additionally, the IPC also wanted to help Health Information Custodians communicate more effectively with the public — *as PHIPA requires custodians to take reasonable steps to inform the public about their information practices and how patients may exercise their rights.*

Health Information Short Notices

- The goal was to develop easy to read items containing the necessary elements regarding the collection, use and disclosure of personal health information, but not to overwhelm individuals with so much information that they will **not** read them;
- The language of the notices must be accessible and easily understood — ***plain language is key.***

Identity Theft

- The fastest growing form of consumer fraud in North America;
- Identity theft is the most frequently cited complaint received by the F.T.C – *40% of total complaints received*;
- 10 million victims of ID theft each year, costing businesses $50 billion, and $5 billion in out-of-pocket expenses from individuals;

— Federal Trade Commission, 2003

The Coming Privacy Storm

- To date, **twenty-three states** have signed laws that now require consumers to be notified if personal information has been subject to a security breach – a further **twenty states** have proposals for such laws;

- Although the new laws are similar to California's SB1386, ***varying state requirements will likely put pressure on Congress to pass a federal version of SB1386;***

- Legislation is also being considered that would ban the sale of Social Security numbers without the permission of the owner, except when needed by law enforcement.

Data-Breach Notification

States Differ on When to Sound the Alarm

- **January 2006**, the Federal Deposit Insurance Corp discovered that stolen personal information from employees was used to set up fraudulent credit union loans;
- Instead of immediately notifying the affected persons, it kept quiet about the breach for a few months at the request of law enforcement;
- The FDIC's experience mirrors that of many banks trying to navigate a mix of security standards spread between federal regulatory guidelines and a host of new state data security laws;
- Further, a number of state laws also conflict with each other, define breaches differently and prescribe different thresholds for notification triggers, for example:
  - **Illinois** does not allow a notification delay for law-enforcement purposes;
  - **Nevada** and **Minnesota** call for alerts whenever an unauthorized breach occurs;
  - **New Jersey** and **North Carolina** do not exempt encrypted data that would be unusable to most identity thieves.

FTC Decisions: *ChoicePoint*

- **February 2005**, personal financial records of more than **160,000** consumers fraudulently obtained; L.A. police believe that the actual number of persons affected could be **500,000**;
- **January 2006**, ChoicePoint fined $10 million in civil penalties by the FTC, the largest in the commission's history;
- An additional $5 million is to be paid in consumer redress to the FTC to settle charges brought against it;
- *"The message to ChoicePoint and others should be clear: Consumers' private data must be protected from thieves. Data security is critical to consumers, and protecting it is a priority for the FTC, as it should be to every business in America."*

— Deborah Platt Majoras, Chairman of the FTC, January 26, 2006.

FTC Decisions:
BJ's Warehouse Club

- **March 2004**, Millions of dollars of unauthorized purchases were made on customer credit and debit cards after customers had visited BJ's stores;

- **June 2005**, the FTC issued a standing order for 20 years.

- Further, a number of financial institutions have filed lawsuits against BJ's seeking the return of about $13 million in fraudulent purchases and operating expenses in connection with the case.

Identity Theft is Easier Than You May Think

- The popular view that identity theft is committed by renegade computer hackers is a myth;
- These crimes continue to depend on a steady and easily accessible supply of personally identifiable information (PII) and are often committed by insiders;
- "…more than 70% of unauthorized access to information systems is committed by employees, as are more than 95% of intrusions that result in significant financial losses."

— Richard Mogul, Senior Analyst with Gartner Group, August 2002.

Privacy By Design
Build It In

- Build in privacy – up front, right in the design specifications;
- Minimize the collection and routine use of personally identifiable information – use aggregate or coded information if possible: data minimization is key;
- Wherever possible, encrypt personal information;
- Use privacy enhancing technologies (PETs): **give your customers maximum control over their data;**
- Assess the risks to privacy: conduct a privacy impact assessment; follow up with privacy audits.

7 Essential Steps for Designing Privacy into Technology

Information and Privacy Commissioner/Ontario
Commissaire à l'information et à la protection de la vie privée/Ontario

1. Define privacy expectations of the public and identify legislated requirements.
2. Develop privacy policies and principles.[1]
3. Undertake an assessment of human and informational resources with a focus on personally identifiable data (collection, processing, management, flows and storage).
4. Undertake a threat risk assessment by completing a Privacy Impact Assessment.[2]
5. Deploy methodology for privacy risk management at the systems level.[3]
6. Introduce the rules and controls developed in the previous step at the source code level.
7. Deploy and audit, through a model of continuous improvement. Review expectations and requirements.

1. Privacy Diagnostic Tool - www.ipc.on.ca/english/[illegible]; Electronic Service Delivery: Privacy Standard - www.gov.on.ca/mbs/english/[illegible]; Code of Fair Information Practices - www.[illegible]

2. Some useful examples of PIA are as follows: Management Board Secretariat's Privacy Impact Assessment - www.gov.on.ca/[illegible].pdf; "The value of Privacy Engineering" by Steve Kenny and John Borking - [illegible].html

3. Methodology should include the development of architecture rules and controls around collection of personal information, linkability, access, use and accountability as well as incorporating the delineation of business processes in terms of [illegible]. The methodology used should be dependent on data type (level of sensitivity etc.).

Privacy By Design:
Tools You Can Use

Privacy Diagnostic Tool

www.ipc.on.ca/userfiles/page_attachments/pdt.pdf

MBS Privacy Impact Assessment

www.accessandprivacy.gov.on.ca/english/pia/index.htm

Electronic Service Delivery (ESD) Privacy Standard

www.accessandprivacy.gov.on.ca/english/pub/esd1.html

Comprehensive Security and Technology

- In many instances, physical access to the data or media is all that is needed for a privacy breach to take place;
- Many security breaches can be avoided if simple physical safeguards had been in place and adhered to;
- However, while physical security measures are important, ***they must*** increasingly be supported by organizational and ***technological reinforcements.***

Don’t Blame the Victim!

- Violations of privacy can be viewed as an external cost – a negative externality;
- Businesses however, not consumers, create privacy externalities through their misuse or lack of sufficient protection of their customers’ personal information;
- It would be far more costly for individuals to prevent, or attempt to remedy, the abuses of their personal information – if possible at all;
- We place the responsibility for protecting customer PII squarely upon business.

Technological Reinforcements

Database Encryption:

- After limiting physical access, the single most important action is to secure data by encrypting it, not just in transit, but also in its place of storage.

Severing or Encrypting Personal Identifiers:

- Encrypt or replace certain sensitive database fields, or otherwise sever the personal identifiers from the data record itself – the transactional data

Data Aggregation, Perturbation and Anonymization:

- Effectively strip away key identifiers and, with them, the ability of data recipients to be able to match and re-identify individual records.

Data Item Masking:

- Mask the sensitive elements of database records (such as PII) from being accessed, transmitted, displayed, printed or otherwise disclosed or modified.

Technological Reinforcements (Cont'd)

Strong Authentication:

- Strong, reliable methods of authentication are necessary to ensure that only authorized individuals, both internal and external, can access and use the data.

Digital Rights Management (DRM):

- DRM can enforce fine-tuned controls over the use and disclosure of data by others, such as their ability to view, copy, print, or forward. DRMs can even auto-delete data or messages not required beyond a specified time period.

Audit Trails / Electronic Tracking:

- A record of all databases accessed should be kept to help detect, deter, and if necessary, prosecute misuse and abuse after the fact – following the data trail is vital.
- Independent third party audit, attestation, and certification may also be desirable for some companies to credibly demonstrate compliance and earn greater trust.

Electronic Audit Trails

- Need to secure client trust and confidence by demonstrating strong governance and accountability framework for entire corporate lifecycle of PII from collection, use, disclosure to disposal;
- Strong detection and enforcement can be filled by automated technology:
  - data-level encryption and rights management technologies;
  - strong authentication and data access control systems;
  - automated keeping and analyzing of network activity logs;
  - real-time, intrusion prevention and detection systems;
- Recording of logs and audit trails are central to all these solutions.

Trust but Verify

The Markle Task Force on National Security in the Information Age issued a paper titled *"Implementing a Trusted Information Sharing Environment: Using Immutable Audit Logs to Increase Security, Trust, and Accountability;"*

Problem:

- Audit logs are maintained in the custody of a systems administrator with authorized access;
- Mutability comes from the systems administrator being able to add, change, and delete log entries;
- Immutable Audit Logs require that:
  1. Log information cannot be altered by anyone regardless of access privilege (thus true immutability); or
  2. That any alterations must be tamper-evident.

Identity Management Systems
PETs

- Privacy Enhancing Technologies (or Tools) 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;
  - manage contactibility or “reachability;”
  - generally, allow users to selectively disclose their PII to others and to exert maximum control over their PII once disclosed.

Identity Management Systems

PETs (cont'd)

- IPC co-published a seminal paper on the subject with the Dutch Data Protection Commissioner in 1997 (www.ipc.on.ca/docs/anoni-v2.pdf);
- Other recent IPC works include guidance on use of PKI, (www.ipc.on.ca/Docs/pki.pdf);

There is currently a significant amount of research and work underway into user-centric identity management systems, notably from:

- EU Privacy & Identity Management in Europe (PRIME - www.prime-project.eu.org);
- EU Future of Identity in the Information Society (FIDIS - www.fidis.net);
- EPrivacy Incorporated Software Agents (PISA consortium www.tno.nl/instit/fel/pisa);
- Microsoft/Kim Cameron (www.identityblog.com);
- Tor: An anonymous Internet communication system (http://tor.eff.org);
- Research by Roger Clarke, Stefan Brands, Ian Goldberg et alia.

Secure Information Destruction
Responsibility and Obligation

- Every organization, whether in the public or private sector, should follow responsible, secure procedures for the destruction of records containing personal information;
- In many cases, it's not just a matter of being responsible, protecting one's reputation, or preventing identity theft – ***it's the law;***
- Several U.S. states such as Georgia, New Jersey and Texas have specific requirements for the destruction of records containing personal information, including when businesses retain disposal companies to dispose of records on their behalf.

Federal Trade Commission
"Disposal Rule"

- On June 1, 2005, new regulations came into effect stemming from the *Fair and Accurate Credit Transactions Act* and outline the duties of persons and companies when disposing of consumer credit reports and information derived from those reports;
- The regulations require "reasonable" disposal measures so that personal information is rendered permanently destroyed;
- Examples of reasonable measures given are burning, pulverizing or shredding such information, and destroying or erasing electronic media containing such information.

Secure Information Destruction: *Need for Industry Standards*

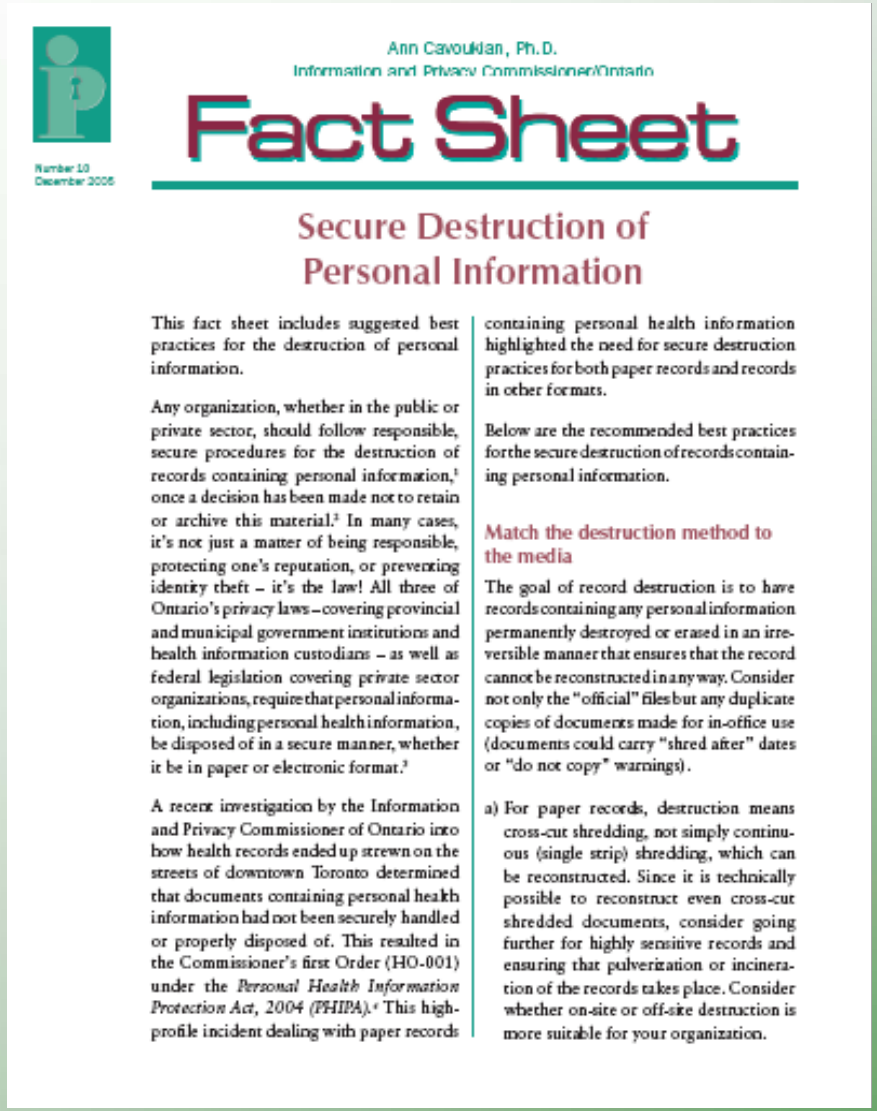
- Industry standards should make clear that secure disposal means permanently destroying the records by irreversible shredding or pulverizing, thus making them unreadable;
- ***Recycling can never be equated with secure disposal;***
- Reliance on a third party to dispose of records must include a written agreement in place setting out the obligation for secure disposal and requiring the third party to provide written confirmation once the secure disposal has occurred.

Secure Information Destruction: *Your Service Provider*

- If you are engaging an external business to destroy records, ***be selective***;
- Look for a provider accredited by an industrial trade association;
- Look for a provider willing to commit to upholding its principles, including undergoing independent audits;
- Look for a provider that will provide a "certificate of destruction;"
- Check references, and insist on a signed contract spelling out the terms of the relationship.

IPC

Secure Destruction Fact Sheet



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

Number 10
December 2006

Fact Sheet

Secure Destruction of Personal Information

This fact sheet includes suggested best practices for the destruction of personal information.

Any organization, whether in the public or private sector, should follow responsible, secure procedures for the destruction of records containing personal information,[1] once a decision has been made not to retain or archive this material.[2] In many cases, it's not just a matter of being responsible, protecting one's reputation, or preventing identity theft – it's the law! All three of Ontario's privacy laws – covering provincial and municipal government institutions and health information custodians – as well as federal legislation covering private sector organizations, require that personal information, including personal health information, be disposed of in a secure manner, whether it be in paper or electronic format.[3]

A recent investigation by the Information and Privacy Commissioner of Ontario into how health records ended up strewn on the streets of downtown Toronto determined that documents containing personal health information had not been securely handled or properly disposed of. This resulted in the Commissioner's first Order (HO-001) under the *Personal Health Information Protection Act, 2004 (PHIPA)*.[4] This high-profile incident dealing with paper records containing personal health information highlighted the need for secure destruction practices for both paper records and records in other formats.

Below are the recommended best practices for the secure destruction of records containing personal information.

Match the destruction method to the media

The goal of record destruction is to have records containing any personal information permanently destroyed or erased in an irreversible manner that ensures that the record cannot be reconstructed in any way. Consider not only the "official" files but any duplicate copies of documents made for in-office use (documents could carry "shred after" dates or "do not copy" warnings).

a) For paper records, destruction means cross-cut shredding, not simply continuous (single strip) shredding, which can be reconstructed. Since it is technically possible to reconstruct even cross-cut shredded documents, consider going further for highly sensitive records and ensuring that pulverization or incineration of the records takes place. Consider whether on-site or off-site destruction is more suitable for your organization.

Provides suggested best practices for the destruction of personal information.

Available for download at:

www.ipc.on.ca/userfiles/page_attachments/fact-10-e.pdf

United States – Examples

United States Department of Health and Human Services:

- *Standards for Privacy of Individually Identifiable Health Information* "Privacy Rule": which implement the privacy requirements of the *Health Insurance Portability and Accountability Act of 1996* (HIPAA);
- The Privacy Rule establishes a set of national standards for the protection of health information, and the use and disclosure of such information by certain health-related service-providers;
- Among other things, the Privacy Rule requires a covered entity to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of health information;"
- In addition, it creates certain obligations on the part of a covered entity that retains a "business associate" (generally, a person or organization outside the covered entity's workforce that provides services involving health information for the covered entity or on its behalf).

United States – Examples *(Cont'd)*

Some states have specific requirements for the destruction of records containing personal information, including when businesses retain disposal companies to dispose of records on their behalf:

- **Georgia**: a business cannot "discard" a record containing a customer's personal information unless it first shreds the record, erases the personal information in the record or makes the personal information unreadable;
- **Texas**: when a business disposes of a record containing a customer's personally identifying information, it is required to make the information "unreadable or undecipherable;"
- **New Jersey**: businesses are required to "destroy, or arrange for the destruction of," records that contain personal information "by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or non-reconstructable."

RFIDs

- RFID technologies have great potential to make our lives more convenient, efficient, and safer;
- However, RFID technologies can also be deployed in privacy-invasive ways;
- Consumer concerns about possible surveillance must be taken seriously by retailers and manufacturers;
- IPC supports use of RFID technologies for use on products, not on people.

IPC RFID Materials:

- *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (February 2004);
- *Guidelines for Using RFIDs in Public Libraries* (June 2004);
- RFID Video (February 2006).

E-Government

- Canada is recognized as a worldwide leader in eGovernment (online government services and programs);
- Canada's Government On-Line strategy continues to set the global standard for delivering targeted and more responsive services to its citizens;
- *"The Internet is providing Canadians greater choice in the way they interact with government and they are increasingly taking advantage of the different options available to them."*

—President of the Treasury Board of Canada, 2003.

E-Government
Canada's Electronic Pass

"E-PASS"

- An E-Pass is a unique electronic credential that allows someone to communicate securely with online-enabled Government services;
- Many of these services require enhanced security measures because they involve exchanging private and personal information over the Internet;
- The Government of Canada, as the service provider, offers unique E-Passes to individuals who choose to use them to access online government services.

How Does a Citizen Get an e-Pass?

1. Citizen tries to access government service and is automatically directed to the ePass token manager's website (still government of Canada);
2. Citizen is prompted to select a username and password;
3. The ePass token manager assigns a meaningless but unique number (MBUN) in association with that username and password;
4. Citizen is then redirected to original government website and inputs username and password to access government services;

Citizen can use the same username and password or create and use unlimited amount of new ones.

E-Government
Meaningless But Unique Number

"MBUN"

- An anonymous digital certificate that allows citizens to encrypt and sign sensitive online transactions with government services;
- **Privacy protected:** No tracking or profiling by the central certification authority because there is no PII associated with an e-Pass certificate.

GO Transit

- **November 2005**, IPC received a complaint under the *Freedom of Information and Protection of Privacy Act* relating to the information collection practices of the Greater Toronto Transit Authority (GO Transit);
- Specifically, the complaint concerns the inappropriate collection of personal information by GO Transit when processing customer cash refunds;
- The attendant processing the refund is required to complete an "Application for Refund" form that requires customers to provide the following information:
  - Name
  - Home address
  - Home and business telephone number
  - Signature

GO Transit (Cont'd)

- In response to this complaint, the IPC initiated an investigation and formed conclusions regarding this information practice:
- Collection of personal information of riders who request a refund **by mail** for any type of ticket **is permissible** under the *Act;*
- Collection of personal information of riders who request a refund **in person is not permissible** under the *Act;*
- The collection of customer personal information for refunds that are processed in person should cease;
- All personal information that had been previously collected in relation to riders who have requested cash refunds should be destroyed.

GO Transit (Cont'd)

- The IPC has also identified several control measures that could be viewed as potential alternatives to the practice of collecting personal information from customers:
  - Requiring that cash refunds be reviewed by a second, more senior employee, at the time the refund is issued;
  - Putting measures in place to ensure that employees engaged in refund transactions do not have access to ticket stock inventory;
  - Separating refund transactions from purchase transactions by requiring customers to go to a separate customer service desk; and
  - Instituting closer monitoring of attendants' transactions to determine the existence of irregularities, through the maintenance of statistics by individual ticket agents on refunds, credits and other non-payment transactions and the identification of unusual trends and anomalies.

Final Thought

"Anyone today who thinks the privacy issue has peaked is greatly mistaken…we are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope."

- Forrester Research, March 5, 2001

How to Contact Us

Commissioner Ann Cavoukian
Information & Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Phone: (416) 326-3333
Web: www.ipc.on.ca
E-mail: commissioner@ipc.on.ca