Secure Privacy

Ken Anderson
Assistant Commissioner (Privacy)
Information and Privacy Commissioner/Ontario

7th Annual ISSEA Conference

May 18, 2006
Marriott Residence Inn, Ottawa

What This Talk Is About

- **Reconciling Science with Privacy**
- **Privacy and the Open Networked Enterprise (O.N.E.)**
- **Designing It/IT in**

Presentation in a Nutshell: Three Key Ideas

- **ICTs are transforming businesses, governments, our worlds**
- **Five major privacy challenges ahead**
- **Skilled IT/IM professionals are needed now more than ever**

Advent of ICTs

- **Welcome to the Information Revolution**
- **"Information Wants to be Free"**
- **"Information is Power"**
- **"Information Needs to Be Managed"**

Growing Information Needs

- Increasingly data-rich activities
- Networks and interdependence
- New models of organization and service
- "Tommy's Terabyte" now a reality

Transformed Business & Government Services

- **More data-intensive activities & services:**
  - **Electronic interaction and Service Delivery**
  - **ICT infrastructure and back-end upgrades**
  - **Law Enforcement initiatives**
  - **Other ambitious, IT projects (EHRs)**

Potential Benefits:

- Better services
- New and more extensive service offerings
- More convenient, personalized, responsive service
- Improved programmatic efficiencies
- Cost savings
- Improved fraud detection
- Greater transparency and accountability
- Enhanced democracy
- Skills upgrades for frontline workers
- Enhanced competitiveness

So What's Holding Up The Great Transformation?

- **#1 Reason: Weak Public Trust and Confidence**

Relentless Negative News:

- **Multi-million $$$ spending failures and boondoggles**
- **High-profile privacy & security breaches**
- **Poor IT security report cards**
- **Insider abuses of personal information**
- **Growing surveillance / access by law enforcement**
- **Controversy or inaction about "new" initiatives**
- **Outsourcing and Patriot Act Issue**

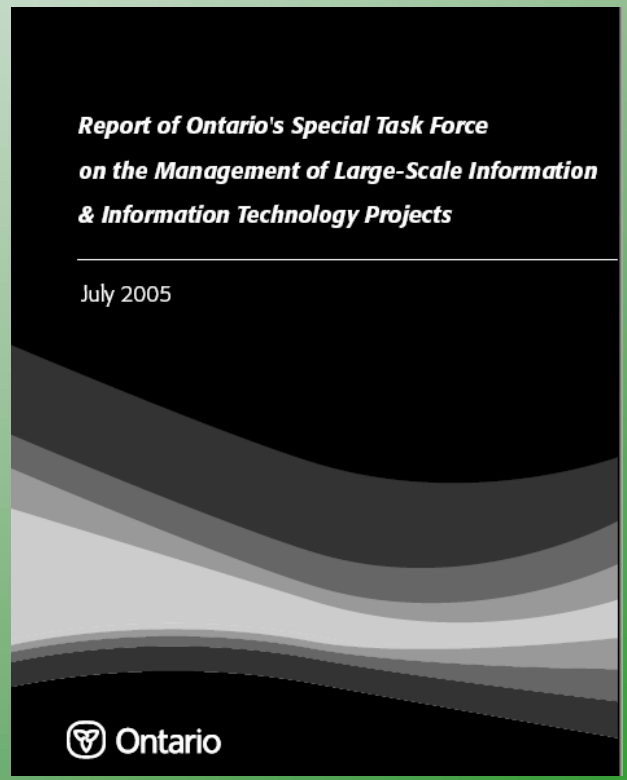
Ontario (Public Sector) Responses:

- Privacy Laws (e.g. FIPPA, MFIPPA, PHIPA)
- Guidance from MGS Access & Privacy Office
- ATIP and Privacy Officers
- IPC/O advice, education and oversight
- GO CPO
- New private-sector privacy law?

Notable documents:

Report of Ontario's Special Task Force on the Management of Large-Scale Information and Key messages

- **Information Technology Projects**
- **Improve governance and accountability**
- **Large IT projects inherently riskier than smaller projects**
- **Large IT projects less about IT, more about business transformation and organizational change**
- **Take time to develop the business case for the project (goals, standards and priorities).**
- **More internal resources needed; project management is a core competency; need for continuity of staffing; leadership**

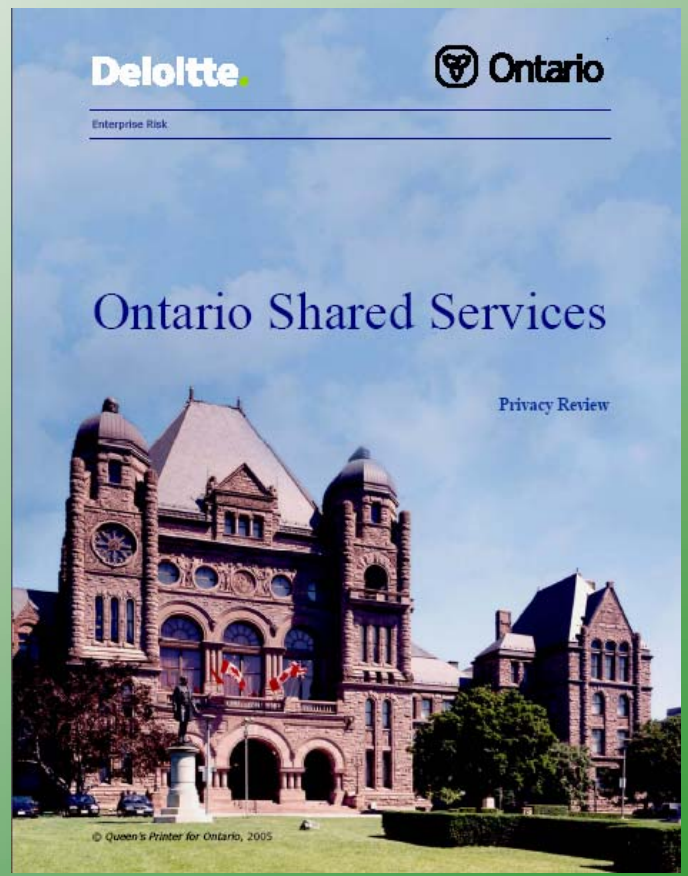


www.mgs.gov.on.ca/english/ministry/releases/nr072805-r.pdf

Notable documents:

SS Privacy Review submitted to IPC Aug/05

- Ontario Government Strengthening Privacy Practices AND Accountability
- Independent, end-to-end audit
- Modified policies and practices
- Better training
- Innovative new “privacy standard”
- Annual audits



www.mgs.gov.on.ca/english/ministry/releases/OSS_Summary_Report.pdf

Objectives: Ensure Public Confidence and Trust

Create strong governance and accountability framework for public sector management of (personal) information in Ontario, including:

- **Establishing strong, clear and effective legal and administrative measures to assure data privacy**
- **Well-published privacy notices, credible promises, documented policies and procedures**
- **Growing community and network of well-trained privacy and information management professionals**
- **Citizen/client confidence and trust**
- **Organizational openness, transparency and accountability – essential ingredients for any effective FOI and privacy program**
- **Responsible and robust management of (personal) information, including mitigating risks and maximizing benefits**

Key Points

- **Personal information (PI) is both an economic asset and a potential liability**
- **Strong data privacy practices are essential to the reputation, profitability and critical business objectives of all organizations**

Informational Privacy: Data Protection

- **Personal control over the collection, use and disclosure of any recorded information about an identifiable individual**
- **The organisation's responsibility for data protection and safeguarding personal information in its custody or control**
- **RC/AC Restricted Collection/Active Containment**

States and Functions of Privacy

States	Functions
• Solitude • Intimacy • Anonymity • Reserve	• Personal Autonomy • Emotional release • Self Evaluation • Limited & protected communication

Privacy vs. Security: Fair Information Practices

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

What Privacy is Not:

Security ≠ Privacy

Privacy vs. Security: The Difference

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation
- Privacy;Data Protection
- Fair Information Practices

- Security
- Organizational control of information through information systems

The Privacy/Security Relationship

- **Privacy relates to personal control over one's personal information**
- **Security relates to organizational control over information**
- **These represent two overlapping, but distinct activities**

Two Key Reasons to Protect Privacy

- **Risk Aversion: Avoiding the negatives**
- **Attracting Opportunity: Good Privacy is Good Business**

General Trends: Privacy & Business

- Information - especially personal information - is the lifeblood of the information economy and of most organizations –public or private- today
- The collection, use and sharing of massive amounts of personal information are becoming subject to greater scrutiny by the public and regulators alike
- Organizations will be punished in the marketplace, and in the courts, for negligent personal information management practices — especially where the costs of their behavior are borne by others (negative externalities)
- Organizations will be rewarded for innovative, far-sighted and diligent information management practices that demonstrate sustained commitment to data privacy principles

All Information is NOT the same!

- **Personal Information ≠ Non-Personal Information**
- **The management of personal information must be completely different than non-personal information**

Old and New

OLD		NEW
Closed decision-making and secrecy	→	Openness, transparency, and accountability
Collect and store as much personal information as possible	→	Collect only what is needed, and keep it no longer than necessary
Personal information is secured at the perimeter	→	Personal information is secured throughout its entire lifecycle
Personal information has economic value that should be exploited	→	Personal information should be managed responsibly with regard for the interests of the customer
The organization decides what is best for the customer	→	The organization asks first for permission, and then involves the customer in a mutually-beneficial trust-based relationship

New Boundaries, New Business Processes

- As companies become internetworked they share new kinds of information
- Organizations are increasingly global
- Business processes are characterized by dense interconnections and constantly evolving relationships
- Modular approach to business affords high degrees of flexibility and adaptation.

Privacy Concerns: Offshoring and Outsourcing

- Third-party data relationships are everywhere now – few organizations can survive in today's world without relying on other firms to help provide, process, or manage data
- As more organizations collaborate, it becomes increasingly difficult for senior management to effectively manage the risk that comes with their organization's ever-growing interdependency with other organizations
- In a business web, information security is only as effective as the weakest link
- Risks are not limited to offshore operations, companies should also determine whether domestic partners observe privacy and security standards

The fundamental issue here is *accountability*.

We suggest:

- Minimize data collection, use, and security risk among partners
- Develop strong contractual agreements and deterrents for third parties
- Deploy continuous monitoring, auditing, and enforcement mechanisms
- Have a realistic privacy crisis management plan in the event of a breach
- Develop a reservoir of client goodwill to draw upon in the event of an incident – clients may be more forgiving

The Modus Operandi of ICT-enabled Organizations is characterized by

- Flatter Hierarchies
- Greater Collaboration
- Devolved Decision-making
- More Risk-taking
- High Flexibility
- Agility
- Adaptability
- Innovation

Privacy Concerns: The Insider Problem vs. Internal Surveillance

- Organizations, in their efforts to ensure security may sometimes engage in what could be perceived as excessive employee surveillance practices
- There has been an increase in employee litigation against companies in reaction to excessive monitoring and surveillance
- A heavily monitored workforce can become less empowered, and lead to resentful employees
- Resentful employees can be a real threat to an organization and its assets, including its information and data assets – beware of rogue employees

The Insider Job

- There are more unauthorized accesses to databases by insiders than corporations admit to their clients, stockholders and business partners, or report to law enforcement
- Approximately 80% of all computer and Internet related crimes are committed by insiders; CSI/FBI Computer Crime and Security Survey
- It is well known that insiders who access databases often have network authorization, knowledge of data access codes, and precise knowledge of the information they want to exploit

We Suggest:

- Appoint and empower a Chief Privacy Officer
- Use technology to automate enforcement of policies
- Develop and implement a privacy awareness and training program

Relationships:

- The success of the ICT-enabled organizations is a often a function of positive experiences and strong relationships with its customers
- Public recognition and word-of-mouth endorsements are among the most valuable types of marketing that any organization can have
- By providing useful, efficient, personalized services and products, the best organizations can foster ongoing trust, loyalty and security; the others will lose customers

Privacy Concerns: Client/Customer Trust

- Peppers & Rogers: The trend towards permission-based marketing is growing in an effort to engage the customer in an ongoing, personalized, 1:1 relationship
- Seth Godin: “Permission-based marketing is just like dating.” — without trust, the relationship cannot develop and flourish
- People are becoming increasingly wary about providing unnecessary information — engaging in the emerging practice of privacy self-defence

Change CRM to "CMR"

- Change the Paradigm: Shift the practice of CRM – Customer Relationship Management, to CMR – Customer Managed Relationships
- Become a customer-centric company: Shift your focus to the customer
- "Nearly 90% of consumers want the right to control how their personal information is used after it is collected." — Forrester Research, 2003

We Suggest:

- Make strong, clear, credible and overt privacy commitments
- Ensure strong consent, access and redress mechanisms are effectively built into information and communications and/or marketing systems

Information Liquidity

- New and rapidly growing industries have arisen whose sole business operation is to collect, analyze and sell personal information, e.g.
- DoubleClick; ChoicePoint; Lexis-Nexis
- The marketplace for personal information is estimated to be in the tens of billions of dollars per year in the U.S. alone
- So lucrative is the information profiling industry that lobby groups have formed to shape the evolution of new privacy and security laws and regulations

Privacy Concerns:
Bad Data, Bad Decisions

Privacy Issues and Liabilities:

- failing to inform, or seek the permission of the clients to obtain personal information from other sources
- failing to get explicit informed consent from clients to share their personal information with third parties
- obtaining and using old or inaccurate data obtained indirectly from third parties

We Suggest:

Ensure that individually identifiable information is:

- legally acquired, used or shared;
- accurate and used for the identified purposes;
- used in a transparent and defensible manner; and
- available for access and correction by the individual

Technology:

- Advances in information and communication technologies now make it possible, on a cost-effective scale never seen before, to collect, store, process, and share vast amounts of highly detailed personal data
- This data comprises our digital shadows, upon which organizations will assess and make decisions for, and about us, often without our knowledge

Privacy Concerns: Over-Collection and Under-Notification

- Just because technology can do it, should it be done?
- It is rare that a technology itself constitutes the privacy risk, but rather, the way in which it is deployed and used by, human decision-makers
- Metro — RFIDs
- ExxonMobil — SpeedPass

Digital Footprints

- Consumer concerns regarding clandestine surveillance and data collection continue to grow
- RFID tags
- Identity and loyalty cards
- Video surveillance
- Biometrics
- Marketing
- DRMs
- Malware

We Suggest:

- Carefully evaluate the legal, PR, and economic risks of adopting any technology-enabled data collection strategy
- Do not hoard data, collect only what is necessary
- Clear privacy policies, prominently displayed and available to individuals at the time of collection
- Meaningful participation, choices and controls to individuals
- Have in place a realistic crisis management plan.

Case Study:

Radio Frequency IDentification

Build privacy early into the design and operation of RFID information systems

- System designers, integrators and commercial adopters take note: tools and techniques are available to minimize the collection and use of personally-identifiable (PII) data in RFID information systems, and to ensure that the promise of “products not people” is fulfilled, e.g.:
- No personally-identifiable information (PII) is ever written to the RFID tags readers cannot “resolve” or associate tag data to PII
- There are built-in controls and limits on access to “lookup” databases
- Read ranges are sharply limited
- Data transactions remain anonymous, or at least pseudonymous
- Interoperability of tags with other RFID systems is circumscribed
- Backend information systems and databases are strongly segregated

Ensure strong security controls on tag data

RFID manufacturers, take note:

Tags can be designed to maximize data protection and security, and to minimize the risks of tag data being "leaked" or misused in an unauthorized manner, e.g.

- tag data can be encrypted, masked or otherwise scrambled
- tags only responds to proprietary readers, using proprietary protocols
- wireless transmission of tag data is done in secure manner
- access to tag data requires additional steps, such as use of password
- meaning and utility of tag data requires additional steps, such as access to lookup database
- tags can be "put to sleep" and/or "awoken" under specified conditions
- tags can be re-purposed for consumers' use and control
- tags can be killed or deactivated in convenient, verifiable manner

Empower Consumers and End-users to Make Privacy Enhancing Decisions and Actions

Consumers, consumer groups, and privacy advocates, take note: technologies and tools exist that can ensure meaningful user involvement, choice and control in the RFID information lifecycle processes. Technology solutions exist to:

- detect the presence and location of both RFID tags and readers
- identify and provide notice of tag contents
- provide audio-visual confirmation of tag data queries, reads, and uses
- assign effective control over tag behaviour to consumers and other end-users
- quickly and easily de-activate tags, either temporarily or permanently
- provide consumers with full access rights to any data associated with a given tag

The specific mix of technological solutions will vary on a case-by-case basis, and there may be some overlap among solutions. The lists above should be considered as a toolkit of privacy-enabling approaches and solutions.

IPC Publications, Guidance and Tools (sample)

- The Security-Privacy Paradox: Issues, Misconceptions and Strategies
- Identity Theft Revisited: Security is Not Enough
- Privacy and Digital Rights Management (DRM): An Oxymoron?
- Privacy-Enhancing Technologies: The Path to Anonymity (Volume I & II)
- Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift
- Incorporating Privacy into Marketing and Customer Relationship Management
- Privacy and Boards of Directors: What You Don't Know Can Hurt You
- Promoting Transparency through the Electronic Dissemination of Information
- Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology

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

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; and
- Recording of logs and audit trails are central to all these solutions

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

- 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
- FTC Disposal Rule

Ok, So Who, Now?

- Lots of work to be done!
- Who's going to solve or manage these problems?
- Short answer: we all are!
- As Information technology professionals
- As citizen/clients
- As mangerial professionals and administrators
- As public lawmakers
- Tasks are richly multi-disciplinary nature, involve:
- Law and regulatory compliance
- Deep understanding of administrative environment, development and deployment of polices and procedures
- Sales, marketing, business development, and communications
- Public and stakeholder relations
- Technology and IT
- Other skills?
- Within the organization: CIO? CSO? CPO? Others?

Who, Now?

We are all information and knowledge-workers, working with data at various points in its organizational life-cycle

- Growing role of the CPO
- Private sector
- Public sector
- Differences between the two
- Need CPOs for large, complex, ambitious IT projects?
- Solid understanding of privacy and how to apply
- Intimate, ongoing knowledge of the organization
- More timely intervention in case of problems
- Better PIAs and more effective follow-up on action items
- Provide a “human face” to the project’s privacy component
- Effective liaison with the IPC
- Improved training and awareness efforts
- More effective internal investigations/complaints management

Who, Now?

- CPO role and functions must be more than window-dressing
- Suitably high-level, independent
- Able to provide strong accountability
- Have broad responsibilities
- Have authority to intervene and take action
- Specialized body of knowledge?
- Multidisciplinary credentials
- Experience a significant asset
- Education and training opportunities
- Emergence of professional groups and associations
- Certification, membership and credentialization opportunities

Who, Now?

Typical CPO responsibilities include:

- develop and put in place comprehensive privacy policy and procedures
- receive and respond to inquiries and complaints;
- carry out audits and investigations;
- mediate and adjudicate privacy issues;
- advise and recommend on corporate strategies, projects, etc.
- conduct / review gap analyses and privacy impact assessments (PIAs)
- issue findings, reports, orders, decisions, etc+
- carry out education, training and awareness initiatives
- provide guidance on key issues
- liaise with government, regulatory, media, business and other groups as appropriate
- help manage public relations exercises and crises

Time is NOW to get on board the privacy rights train, upgrade your skills, and be part of the privacy enhanced solution not the privacy-invasive problem.

RECAP:

- Organizations – public and private sector are being transformed by ICTs
- The development and operation of the ICTs must be carried out in a privacy-enabled, if not enhanced manner
- Good privacy laws, tools and other mechanisms exist
- Major privacy challenges lie ahead for all organizations – public or private – that must adapt to the new information and technology-rich environment
- Needed right now are qualified people to ensure that the privacy challenges are met head-on and consistently.
- Time is NOW to get on board the privacy rights train, upgrade your skills, and be part of the privacy enhanced solution not the privacy-invasive problem.

How to Contact Us

Ken Anderson
Assistant Commissioner (Privacy)
Information & Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Phone: (416) 326-3942
Web: www.ipc.on.ca
E-mail: ken.anderson@ipc.on.ca