Embed Privacy Into Your IT Business Practices: Municipalities Can Reap Significant Gains

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

Greater Toronto Marketing Alliance
Municipal Information Systems Association
Ontario Public Buyers Association
April 27, 2009

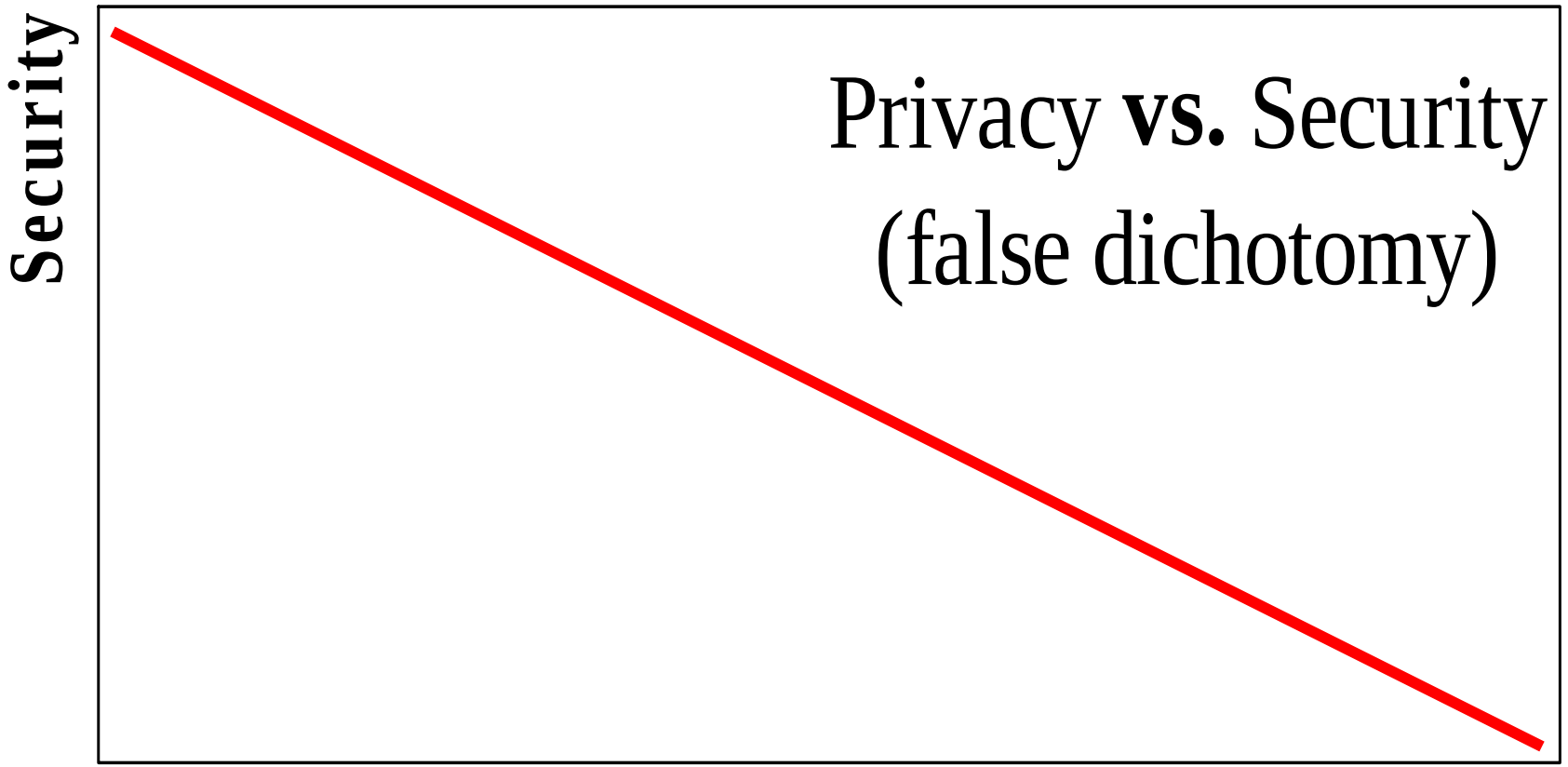
Presentation Outline

1. *The Future of Privacy: Positive-Sum NOT Zero-Sum*
2. *Privacy by Design: Build It In*
3. *Why Privacy is Good for Business*
4. *Managing Your Data: Secure Data Destruction*
5. *Privacy in the Clouds: Networked Computing*
6. *Doing Business with Government: An Open and Transparent Procurement Process*
7. *Conclusions*

The Future of Privacy:

Positive-Sum
NOT
Zero-Sum

Privacy OR Security:
A Zero-Sum Game



We Need to

Change

The Paradigm

Positive-Sum Paradigm

- A **Zero-Sum Paradigm** describes a concept or situation in which one party's gains are balanced by another party's losses – win/lose; either/or; enhancing security often comes at the expense of privacy – the more you have of one, the less you can have of the other;
- A **Positive-Sum Paradigm**, in contrast, describes a situation in which *all* participants may gain together (win-win);
- To achieve a positive-sum model, privacy must be proactively built into the system so that privacy protections are engineered directly into the technology, right from the outset;
- The effect is a minimization of the unnecessary collection and use of personal data by the system, while at the same time, strengthening data security, and empowering individuals to exercise greater control;
- This can result in technologies that achieve strong security *and* privacy, delivering a "win-win" outcome.

Positive-Sum Model

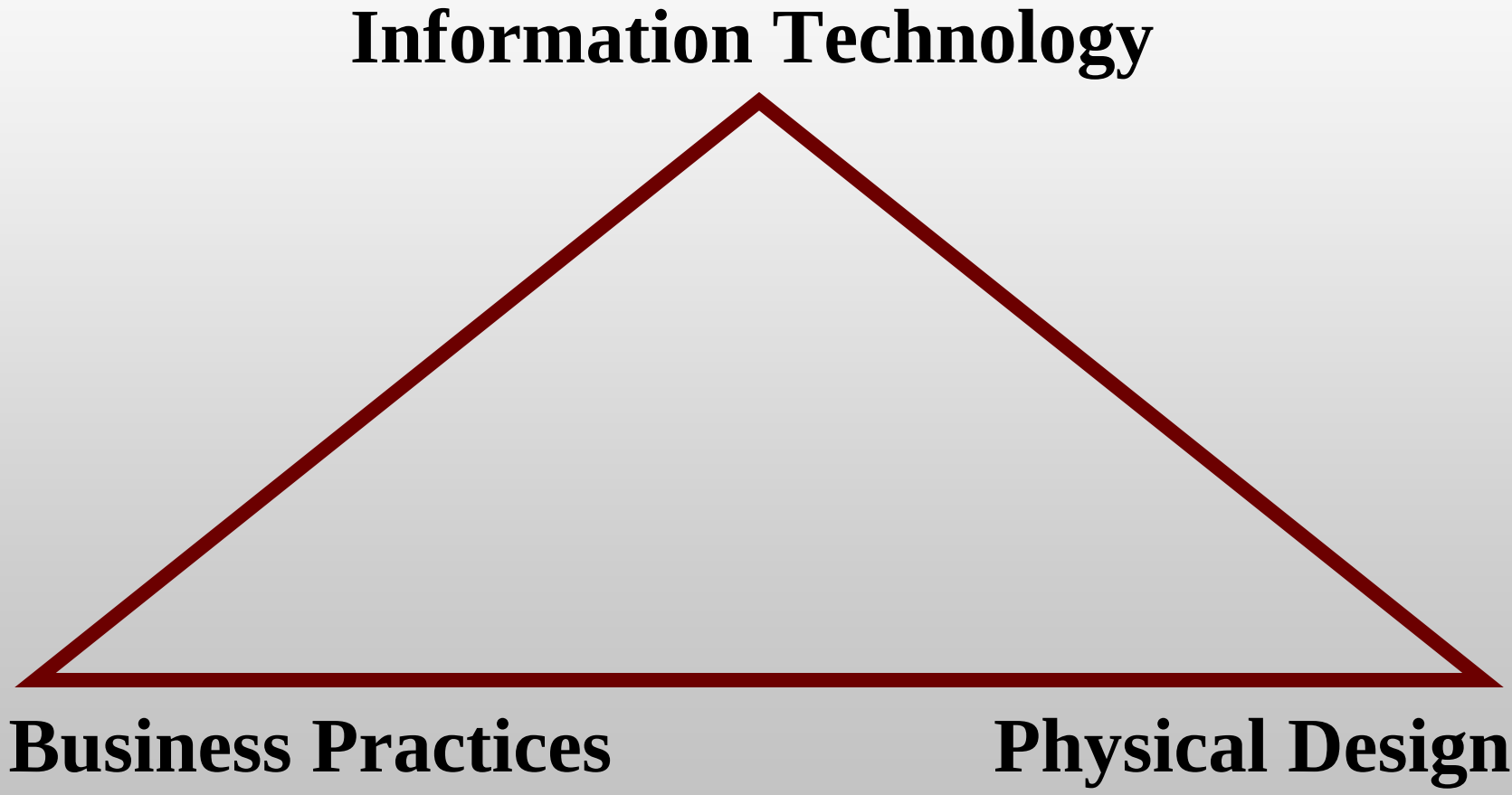
Change the paradigm from a zero-sum to a positive-sum model: Create a "win-win" scenario, not an "either/or" involving unnecessary trade-offs

Privacy by Design: Build It In

Privacy by Design: "Build It In"

- I first developed the term "Privacy by Design" in the 1990's, 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 right 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 privacy-enhancing technologies (PETs) where possible: give people maximum control over their own data.

Privacy by Design:
The Trilogy of Applications



Why Privacy is Good for Business

The Bottom Line

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

Think of privacy as a sound business strategy

Costs of A Privacy Breach

- Legal liabilities, class action suits;
- Loss of client confidentiality and trust;
- Diminution of brand and reputation;
- Loss of customers, competitive edge;
- Penalties and fines levied;
- Costs of crisis management, damage control, review and retrofit of information systems, policies and procedures.

Managing Your Data:

Secure Data Destruction

Managing Your Data

- Does your organization have a Data Map?
- Do you know all the sources of personally identifiable information (PII) in your organization?
- Do you know how customer data flows throughout your organization?
- Do you have a consent management system in place (when you need to obtain additional consent from your customers)?

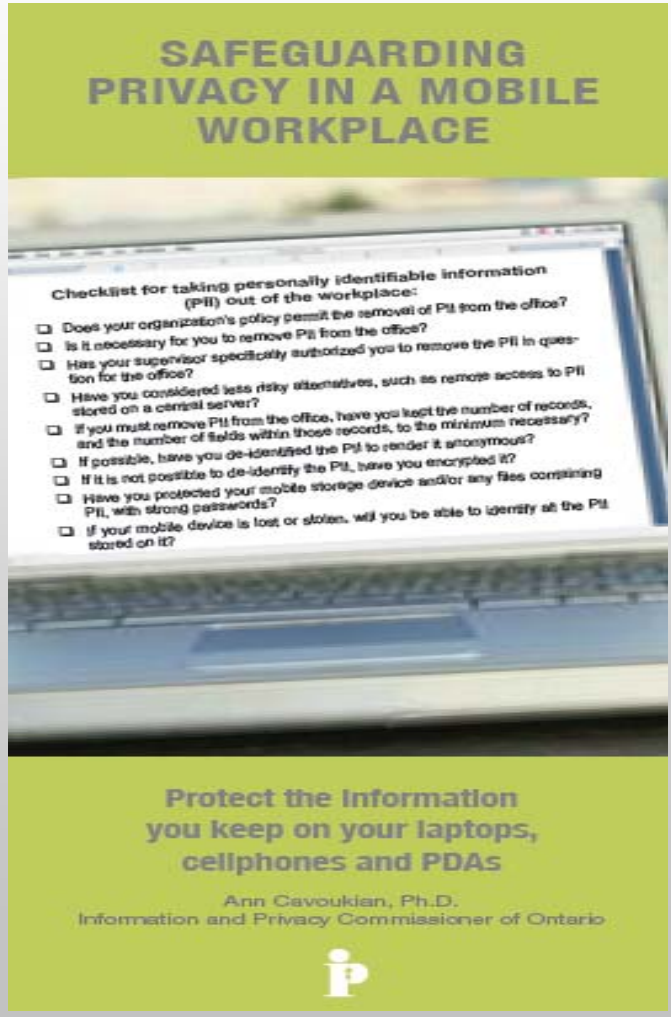
Portable Devices

Working away from the “bricks and mortar” office also means working outside the traditional security layers. Result: additional steps must be taken to safeguard confidential information.

Brochure on Mobile Devices

Safeguarding Privacy In A Mobile Workplace

- Does your organization's policy permit the removal of PII from the office?
- Is it necessary for you to remove PII from the office?
- Has your supervisor specifically authorized you to remove the PII in question for the office?
- Have you considered less risky alternatives, such as remote access to PII stored on a central server?
- If possible, have you de-identified the PII to render it anonymous?
- If it is not possible to de-identify the PII, have you encrypted it?
- If your mobile device is lost or stolen, will you be able to identify the PII stored on it?



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

Fact Sheet

Wireless Communication Technologies: Safeguarding Privacy & Security

- A good starting point for understanding the impact of technological change is to regularly re-examine past assumptions and decisions;
- Any time wireless technology is used to transmit personal information, that information must be strongly protected to guard against unauthorized access to the contents of the signal.

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

Fact Sheet

Number 14
August 2007

Wireless Communication Technologies: Safeguarding Privacy & Security

We are fast approaching the point where it is reasonable to assume that any device that creates or stores data either has, or is connected to, some form of embedded wireless capability. Cell phones and personal digital assistants (PDAs) are increasingly sophisticated, often combining multiple wireless technologies in a single device.

Wireless technologies can reduce costs, increase efficiencies, and make important information more readily and widely available. In the health care sector, for example, wireless data communications now make it possible for paramedics to send cardiac images and data directly to cardiologists, significantly reducing wait time to treatment.

Clearly, the benefits of wireless communications are many. But, there are also risks. Without appropriate safeguards, transmitting data wirelessly can be like using an open filing cabinet in a waiting room. In fact, this Office just recently issued an Order about a case where unauthorized viewers had inadvertently intercepted wireless video images of patients in a washroom providing urine samples.

This Fact Sheet addresses privacy issues arising from the use of wireless technologies, expanding on Fact Sheet #13, *Wireless Communication Technologies: Video Surveillance Systems.*

Taking Care

The *Personal Health Information Protection Act* (PHIPA), the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) set out requirements for the protection of personal information, including information in electronic form.

In general, compliance with these *Acts* requires that those responsible take reasonable measures to protect personal information, which may include physical safeguards, using role-based access to personal information, or technological measures such as encryption.

The transmission of personal information in electronic form, particularly through the use of wireless technologies, means adding "data-in-motion" to "data-at-rest" as a category of data to protect, and adds another layer of complexity to compliance with these *Acts*.

A good starting point for understanding the impact of technological change or new developments is to regularly re-examine past assumptions and decisions. A reasonable precaution is one that any prudent and privacy conscious individual or institution would take. For example, there was a time when it was reasonable to browse the web and download files without

www.ipc.on.ca/index.asp?navid=46&fid1=645

Secure Data 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;***
- Industry standards should make clear that secure disposal means permanently destroying the records by irreversible shredding or pulverizing, thus making them unreadable;
- ***Recycling should never be equated with secure disposal.***

Fact Sheet:

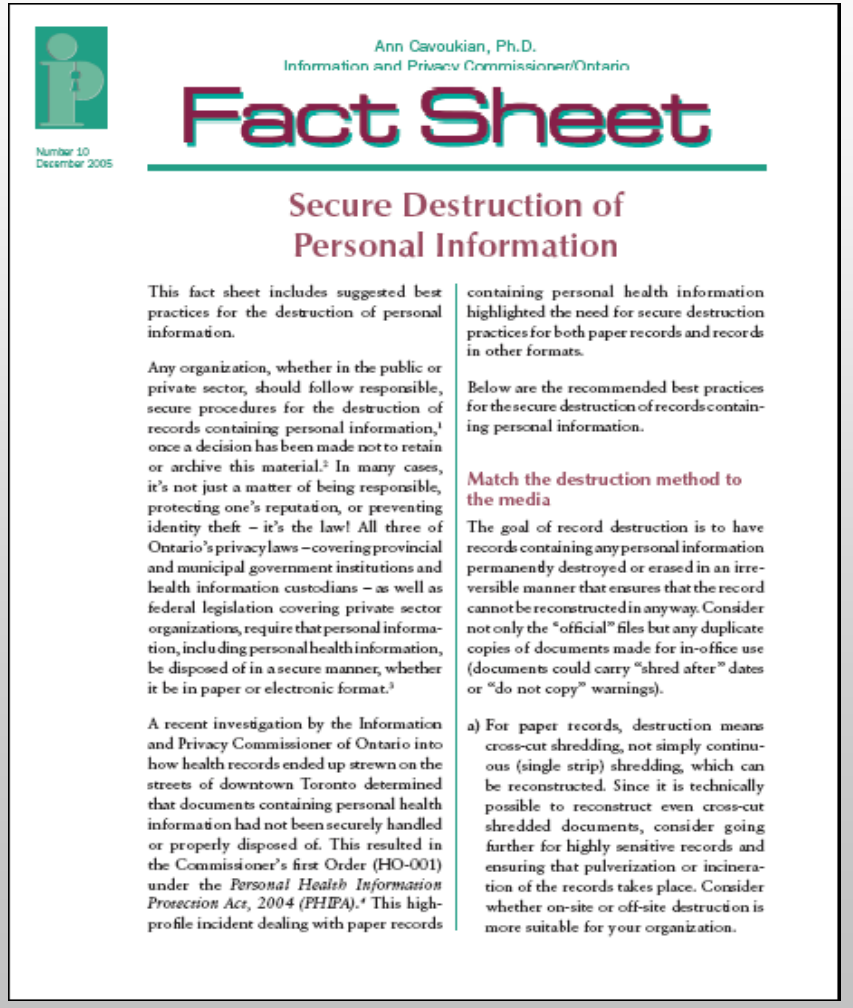
Secure Destruction of Personal Information

Match the destruction method to the media:

- The goal of secure records destruction is to permanently destroy or erase personal information in an irreversible manner;

Select and engage your service provider with due diligence:

- Be selective. Look for a provider who is accredited or is willing to commit to upholding its principles, including undergoing independent audits.



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

Number 10
December 2005

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.

www.ipc.on.ca/images/Resources/up-fact_10_e.pdf

Outsourcing Records Destruction

"You can outsource services … but you can't outsource Accountability. You always remain accountable."

- Dr. Ann Cavoukian,
Information and Privacy Commissioner of Ontario

Secure Data 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.

Privacy Data Breaches: A Few Low-Tech Solutions

- Keep an inventory (a data map) of all PII collection points, uses, assets, and disclosures in your organization - you cannot protect what you don't know exists;
- Securely destroy unnecessary PII, regardless of the media – ***recycling is not a form of secure destruction;***
- Consider the services of external privacy and security auditors and certification programs - especially when "outsourcing;"
- Vet employees with access to personal information - including all temporary, part time employees and outside contractors;
- Train all staff to recognize privacy threats and to respond appropriately – ***create a culture of privacy in your organization****;*
- **Breach Notification:** When faced with a breach, lead with openness and transparency: Contain the damage, notify affected parties, fix the problem.

Privacy in the Clouds: Networked Computing

IPC
www.ipc.on.ca

Privacy in the Clouds

Evolution of Consumer Computing:

1. **The stand-alone PC** in which the user's software and data are stored on a single, easily protected machine, such as word processing, spreadsheets;

2. **The Web** in which most of the software a user needs is still on their own PC, but more and more of the data they need is found on the Internet, such as a Web browser;

3. **The "Cloud"** in which users rely heavily on data and software that reside externally on the Internet. Examples: using Google Apps for word-processing; virtual worlds such as Second Life that enable users to build 3D environments combining Web pages and Web applications.

   See *The Information Factories* by George Gilder, Wired magazine, October, 2006, www.wired.com/wired/archive/14.10/cloudware_pr.html

The Power and the Promise of Cloud Computing

- **Limitless flexibility**: With access to millions of different pieces of software and databases, and the ability to combine them into customized services, users are better able to find the answers they need, to share their ideas, and enjoy online games, video, and virtual worlds;
- **Better reliability and security**: Users no longer have to worry about their hard drives crashing or their laptops being stolen;
- **Enhanced collaboration**: By enabling online sharing of information and applications, the Cloud offers users new ways of working and "playing" together (think social networks);
- **Portability**: Users can access their data and tools anywhere that they can connect to the Internet;
- **Simpler devices**: With data and the software being stored in the Cloud, users no longer need a powerful computer. They can interface using a cell phone, a PDA, a personal video recorder, an online game console, their cars, or even sensors build into their clothing.

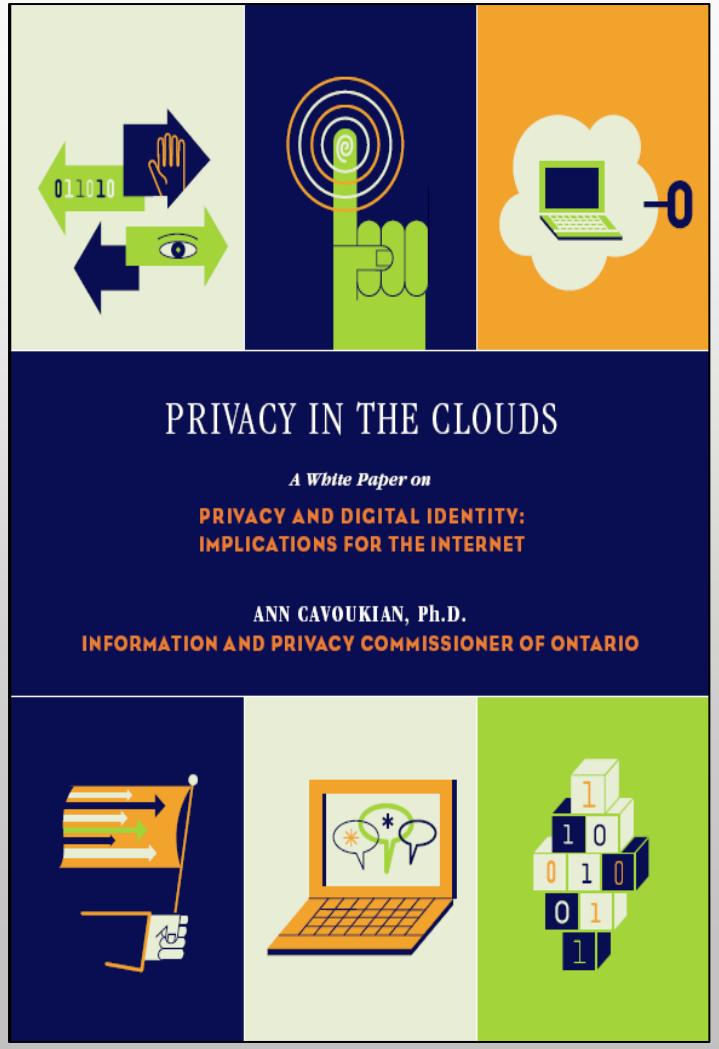
The Digital Identity Needs of Tomorrow

- What is needed – ***flexible*** and ***user-centric*** identity management:
- ***Flexible*** to support the multitude of identity mechanisms and protocols that exist and are still emerging, and the different types of platforms, applications and service-oriented architectural patterns in use;
- ***User-Centric*** because end users are at the core of identity management – they must be empowered to execute effective controls over their personal information;
- A truly flexible identity management system would not be limited to laptop and desktop computers; it would also work on cell phones, PDAs, consumer electronics like video recorders and online game consoles — any way a user might touch the Internet.

Privacy in the Clouds
(in the Web 2.0 World)

Cloud Building Blocks:

1. Open source and proprietary identity software based on open standards;
2. Federated Identity;
3. Multiple and partial identities;
4. Data-centred policies;
5. Audit tool.



www.ipc.on.ca/images/Resources%5Cprivacyintheclouds.pdf

Federated Privacy Impact Assessment (F-PIA)

Goals of an F-PIA:

- Provide an opportunity for members to develop and codify a Federation's privacy policies;
- Demonstrate that privacy policies, as defined by members of the Federation, will be met;
- Demonstrate that an appropriate technological architecture is in place to prevent, to the extent possible, accidental or malicious violations of privacy policies.

Doing Business with Government: An Open and Transparent Procurement Process

An Open and Transparent Procurement Process

- In my 2005 annual report, I highlighted the need for public accountability in the expenditure of public funds with a focus on government procurement processes;
- Ensuring the integrity and effectiveness of any government procurement process was the basis of my recommendation that contracts entered into by government institutions be made public on a routine basis;
- In 2006, I went a step further and called upon government organizations to make the full procurement process even more transparent – releasing information not only on the winning bid, but for all bids.

Benefit of an Open Process

- The commercial benefits of an open bidding process were also recognized in a report by the ***Doing Business with the Ontario Government Task Force***, released in January 2006; **www.gov.on.ca/mgs/en/AbtMin/STEL02_047060.html**
- The Ontario government established the Task Force to:
  - Ensure that government operations were efficient and effective with respect to the bidding process; and
  - Study government procurement policies and processes to help enhance access for small and medium-sized businesses to government procurement opportunities;
- This is what I would call a **"win/win"** scenario. Increased government transparency *and* more opportunities for companies to do business with government.

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
Section 10(1)

For section 10(1) to apply, the appellant must satisfy each part of the following three-part test:

1. The record must reveal information that is a trade secret or scientific, technical, commercial, financial or labour relations information; and

2. The information must have been "supplied" to the institution "in confidence," either implicitly or explicitly; and

3. The prospect of disclosure of the record must give rise to a reasonable expectation that one of the "harms" specified of section 10(1) will occur.

www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm

Order MO-2283
City of Oshawa

- The City of Oshawa received a request under *MFIPPA* for access to pre-qualifications, qualifications, and proposals submitted by a consortium to the City of Oshawa with respect to a proposed downtown sports and entertainment facility;
- The City denied access under section 10(1)(a) which is designed to protect the confidential "informational assets" of businesses or other organizations that provide information to government institutions;
- However, section 10 does not provide blanket privacy coverage for every aspect of a company's business;
- This Order directed that most of the information be disclosed with only a very limited amount of specific financial and commercial information remaining confidential.

www.ipc.on.ca/images/Findings/mo-2283.pdf

Order MO-2117
City of Windsor

- The City of Windsor received an access request for a copy of an agreement for parking spaces in the municipal garage attached to a building relating to spots designated for a particular company;
- The City denied the request citing that the lease terms were supplied in "confidence" and that the affected party requires the information be kept confidential in order to maintain a competitive position relative to other potential tenants in the facility;
- After careful examination, the IPC came to the conclusion that the terms of the contract did not qualify as having been "supplied" stating that agreed upon terms of a contract are considered to be the product of a negotiation process (not a trade secret) and therefore can not be considered as having been "supplied."

www.ipc.on.ca/images/Findings/up-mo_2117.pdf

Order MO-2093
City of Hamilton

- The City of Hamilton received a request for copies of successful bids and scoring results regarding three companies that won bids to supply the city with computer equipment and services;
- While the City did release information for two of the successful bidders, it denied full disclosure regarding the third successful bid stating that the information could be considered protected under section 10(1) of *MFIPPA* as it contained technical, financial and intellectual property information;
- While my office did find that some of the information was technical and financial in nature, it did not support the argument that countless hours of implementing best practices and industry knowledge, in addition to service response times, extended warranty options, unique value propositions and maintenance contracts could be considered as "intellectual property."

www.ipc.on.ca/images/Findings/up-mo_2093.pdf

Conclusions

- Lead with privacy by design – change the paradigm from a zero-sum game to a positive-sum model, where both privacy *and* security are embedded directly into the technology;
- When you change the paradigm, you think differently: Make it privacy *AND* security, not the mutually exclusive "either/or;"
- Build privacy into your business practices and operations – positive-sum, all the way;
- Follow responsible, secure procedures for the destruction of records containing personal information – recycling should never be equated with secure disposal – they are not the same;
- You can outsource services … but you can't outsource accountability. You always remain accountable;
- Bottom line: treat privacy as a business issue, not a compliance issue; it makes good business sense.

How to Contact Us

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca