

***Access & Privacy:
Challenges and Opportunities***

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario**

**Ministry of Government Services
Access and Privacy Workshop 2009
*October 26, 2009***



Access to Information



Right to Know Week – 2009


- Last month, my office sponsored the fourth annual *Right to Know Week* in Canada by sending teams to three Ontario cities with information tables and handouts of IPC publications;
- IPC staff also held presentations to media students at a number of Ontario universities and community colleges on how journalists can make good use of freedom of information laws;
- We also posted information on a special *Right to Know* section of our website (www.ipc.on.ca) about: access to government information; how to file FOI requests; how to file appeals; and an FOI quiz.

www.righttoknow.ca/home/index_e.php



Making it clear that all Ontario universities are subject to *FIPPA*

- The Ontario Government amended the *Freedom of Information and Protection of Privacy Act* to bring universities under the legislation as of June 2006;
- My office strongly encouraged the government to bring in such legislation as universities receive funding from the government which brings them within the scope of *FIPPA* – Regulation 460;
- However, I discovered that a gap remains;
- The case in point dealt with a freedom of information request to Victoria University, an institution that is federated with the University of Toronto and is not listed under Regulation 460.



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

News Release May 13, 2009

Commissioner Cavoukian lays out path for increased privacy protection & accountability –

TORONTO – Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, is urging the provincial government to make specific legislative changes and take additional steps to protect privacy and ensure greater accountability.

In her 2008 Annual Report, released today, the Commissioner cites how her sweeping recommendations from her seminal investigation into a privacy complaint against the video surveillance program of Toronto's mass transit system have been hailed in the United States as a model that cities around the world can build upon, and in Canada as "a road map for the most privacy-protective approach to CCTV."


Among the recommendations she is making in her 2008 Annual Report, are:


- **Amend the law to make it clear that all Ontario universities fall under *FIPPA*.**

The Commissioner is calling on the government to fix a potential omission in the *Freedom of Information and Protection of Privacy Act* related to which organizations are covered under the *Act*.

Under amendments that came into force in mid-2006, publicly funded universities were brought under the *Act*. Due to the wording of an amended regulation, the University of Toronto, in response to a freedom of information request received under the *Act*, argued that Victoria University, an affiliated university, was not covered under the *Act*.

"An IPC adjudicator determined that, based on the financial and academic relationship between the two, Victoria was part of the University of Toronto for the purposes of *FIPPA*," said Commissioner Cavoukian. "The University of Toronto has not accepted our ruling and is now appealing it – having it 'judicially reviewed.' They have chosen to fight openness and transparency, expending valuable public resources in the process. We find this completely unacceptable, which is why we are prepared to go to battle on this issue, in our effort to defend public sector accountability. We should add that this is contrary to our normal process of working co-operatively with organizations to mediate appeals and resolve complaints informally. In this case, however, the university, having thrown down the gauntlet, left us no choice but to respond in kind and aggressively defend our Order in the courts."

 2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A6

 2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A6

416-976-3333
1-800-387-0073
Fax: 416-325-8186
TTY: 416-325-7539
<http://www.ipc.on.ca>



Make it clear that all Ontario universities are subject to *FIPPA*

(Cont'd)

- While an IPC adjudicator concluded that Victoria University was subject to the *Act* – there are still more than 20 other affiliated and federated universities in the province;
- The government needs to amend the regulation relating to this, in order to avoid future questions about whether affiliate universities are covered by the *Act*;
- There is no principled basis for affiliated and federated universities not being subject to the province's access to information and privacy regimes – the need for accountability for the expenditure of public funds remains the same;
- The exclusion of any federated or affiliated university from the *Act* simply through an anomalous relationship with the parent university would be an unacceptable result – one that can be easily avoided through the enactment of an amendment to the Schedule of Institutions in Regulation 460.



High Profile Appeal:

Ontario Lottery and Gaming Corporation

- My office, ordered the Ontario Lottery and Gaming Corporation (OLG) to disclose records pertaining to its investigations verifying significant lottery wins by lottery ticket retailers;
- With the exception of certain information about their ethnic origin, the OLG's decision to deny access to portions of the records containing the personal information of winners was not upheld in the Order;
- My office balanced the privacy interests of the insider winners against the need for public scrutiny of the OLG's lottery operations and concluded that the records ought to be disclosed;
- Factors favouring the disclosure of the information outweighed those in favour of privacy protection – the public scrutiny consideration in section 21(2)(a) of the Freedom of Information and Protection of Privacy Act was heavily relied upon.



Landmark Court Ruling: *Toronto Star vs. Toronto Police*

- The Toronto Star filed freedom of information requests with Toronto Police, seeking data on arrests and occurrences, with personal identifiers removed;
- The police refused and the Toronto Star filed an appeal with the IPC which resulted in an Order;
- The police challenged the IPC Order and applied for judicial review to Ontario's Divisional Court, which overturned the IPC's Order;
- The Divisional Court's ruling was eventually overturned by the Ontario Court of Appeal under the *Municipal Freedom of Information and Protection of Privacy Act*;
- This case represents a victory for openness and transparency in the context of electronic records – welcome to the 21st Century!



News release

January 13, 2009

Landmark court ruling hailed by Commissioner Cavoukian as upholding openness and transparency of electronic records

TORONTO – A ruling handed down by the Ontario Court of Appeal today is “a landmark decision that upholds the principles of openness and transparency as applied to electronic records,” said Ontario Information and Privacy Commissioner Ann Cavoukian.

The Court allowed appeals by the IPC and a Toronto Star reporter from a Divisional Court ruling and restored the IPC's Order applying the definition of “record” in section 2 of the *Municipal Freedom of Information and Protection of Privacy Act* to electronic databases maintained by the Toronto Police Services Board. In that Order, the IPC held that the need to develop a computer program to anonymize personally identifiable information held in the databases would not result in the creation of new records outside the scope of Ontario's freedom of information legislation.

In its ruling today, the Court directed the Toronto Police Services Board to respond to the Star's requests immediately and to pay the newspaper's legal costs.

The Star originally filed two freedom of information requests with the Toronto Police, seeking information from the police databases of arrests and occurrences, with personal identifiers removed, for its series of articles on racial profiling. When the Star was not able to obtain the information it sought, it filed an appeal with the IPC. The position taken by the police – that the information sought was not a “record” – was rejected by the IPC, which ordered the police to make a decision on access to the information.

The police then challenged the IPC Order and applied for judicial review to Ontario's Divisional Court, which overturned the IPC's Order, holding that the need to develop new software takes the request outside the statutory definition of “record.”

Today, the lower court decision was reversed. In its far-reaching decision, the Court of Appeal, Ontario's highest court, agreed with the IPC's submissions that the definition of record must be read “subject to the regulations,” which contemplate that institutions may be required to develop new computer programs to respond to requests. Because the Toronto Police Services Board had the technical expertise to develop an algorithm using its current software to create the requested records, the request satisfied the definition of record and upheld the IPC's initial decision.

“This case,” said Commissioner Cavoukian, “represents a victory for openness and transparency in the context of electronic records – welcome to the 21st Century!”

Here is a direct link to the Court of Appeal ruling:
<http://www.ontariocourts.on.ca/decisions/2009/january/2009ONCA0020.htm>

Media Contact:
Bob Spence
IPC Communications Co-ordinator
Direct line: 416-326-3939; Cell phone: 416-873-9746; Toll free: 1-800-387-0073;
bob.spence@ipc.on.ca



2 Brock Street East
Suite 1400
Toronto, Ontario
M9W 1A8

2, rue Brock est
Bureau 1400
Toronto (Ontario)
M9W 1A8


416-326-3333
1-800-387-0073
Fax/Télé: 416-326-9199
TTY: 416-326-7039
<http://www.ipc.on.ca>



County of Simcoe – Site 41

First Order – *MO-2416*

- A new landfill site being developed by Simcoe County, known as “Site 41” is facing vigorous opposition from residents in surrounding communities;
- A freedom of information request was filed to obtain data from a hydrogeological model prepared by engineering consulting firm Jagger Hims;
- **May 13, 2009** – I ordered the Simcoe County to issue a written direction to Jagger Hims requiring that the records in question be delivered to the County;
- The County failed to comply with this initial order by indicating that it was not willing to take any additional actions to obtain the data – *I found this to be completely unacceptable.*




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

ORDER MO-2416

Appeal MA07-365

County of Simcoe



Tribunal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services de Tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8


Tel: 416-326-3333
1-800-387-2073
Fax/Tel: 416-325-0150
TTY: 416-325-7530
http://www.ipc.on.ca



County of Simcoe – Site 41

Second Order – *MO-2449*

- Following Simcoe County’s refusal to comply with the first Order, I issued a subsequent Order directing the County to take all steps, including legal proceedings if necessary, to obtain the model and input data from Jagger Hims;
- The fact that Jagger Hims received and used taxpayer money to create the model and input data gives the County a potent legal basis for compelling the firm to provide the County with these records;
- At the heart of the matter is a complete absence of what I call *Access by Design* – when institutions embark on ventures that will have major implications to the public they must plan up-front to include access to information of public interest.



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

ORDER MO-2449

Appeal MA07-365

County of Simcoe

Tribunal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services de Tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Tel: 416-326-4160
TTY: 416-326-7538
http://www.ipc.on.ca



A More Open and Transparent Procurement Process

- I have called for increased openness and transparency when it comes to government contracts;
- Government institutions and private sector businesses need to be aware that section 17 of *FIPPA* does not offer “blanket coverage” in providing exemptions from disclosing information;
- Often in the past, government institutions have automatically granted section 17 exemption to any material received from a third party, including contracts;
- IPC Orders have consistently stated (with some exceptions) that these contracts are not subject to section 17 and must be disclosed;
- Anecdotally, the IPC is seeing fewer cases where section 17 is being claimed by government institutions for contracts.



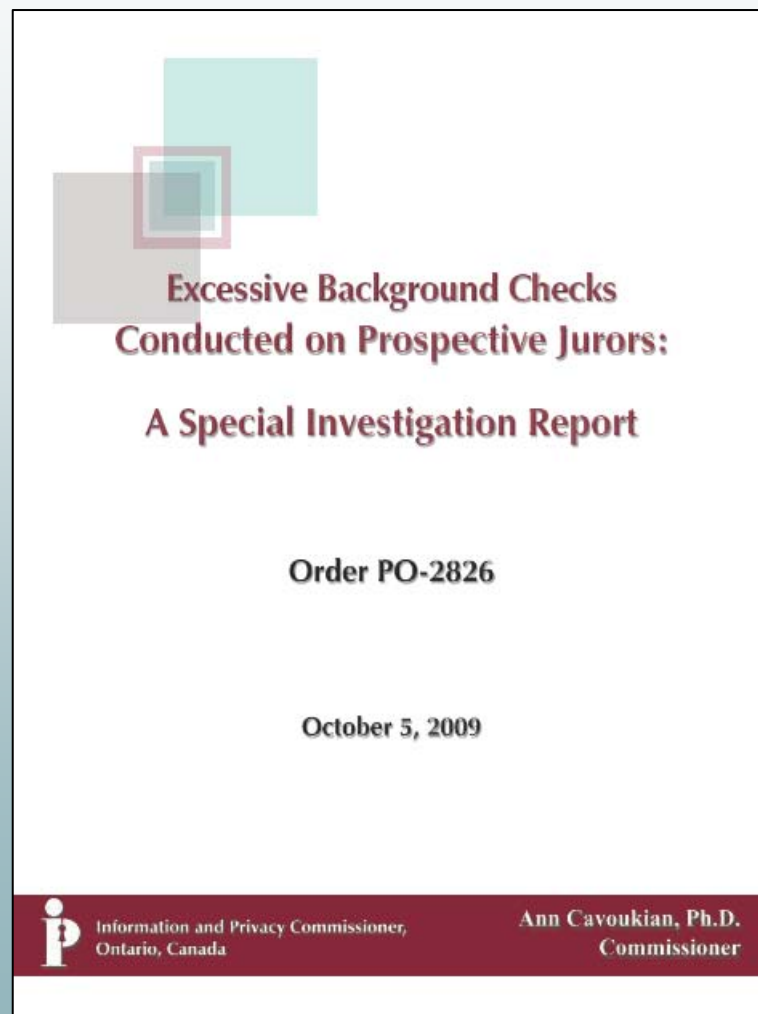
Privacy



Juror Screening Report

Order PO-2826

- **May 25, 2009** – a report in the media indicated that background checks were being conducted on prospective jurors;
- Once the possibility arose that this practice went beyond an isolated incident and that it could be widespread, I felt compelled to launch an investigation;
- In my Order, I directed Crown attorneys to cease the collection of personal information about prospective jurors that does not directly relate to the *Juries Act* or *Criminal Code* eligibility criteria;
- In addition, I also made 22 recommendations that will lead to the creation of a single juror screening system.





Juror Screening Report

Recommendations

Among my 22 recommendations:

- The Ministry of the Attorney General (MAG) through its Provincial Jury Centre (PJC), should be the only central body to screen jurors who are ineligible for jury duty, based on criminal conviction;
- Crown attorneys should cease the practice of requesting the police to provide criminal conviction information relating to potential jurors, barring exceptional and compelling circumstances;
- Where Crown attorneys do obtain criminal conviction information relating to prospective jurors, they should share this information with defence counsel, in accordance with MAG policy;
- MAG should re-write and re-design the jury service qualification questionnaire in order to make it more clear, transparent and user-friendly for all prospective jurors;
- MAG should develop and implement a policy for Crown attorneys on the appropriate retention and disposal of jury panel lists.



High Profile Privacy Incident: *Toronto Hydro Breach*

- In July, 2009, Toronto Hydro discovered a major privacy breach:
 - Hacker fraudulently set up E-bill accounts which allow customers to view their bill online;
 - All customers notified by letter and breach was reported to IPC;
 - Police investigation underway;
 - Interval investigation proceeding;
- IPC investigation to determine cause of breach and whether adequate safeguards exist is ongoing.



News Release

Date: July 28, 2009

Commissioner Cavoukian investigating online privacy breach at Toronto Hydro

TORONTO – Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, has launched an investigation into a privacy breach of Toronto Hydro's e-billing system.

The IPC has been working with Toronto Hydro since last Friday, when the Commissioner's office was first advised of the privacy breach. The breach had been discovered earlier in the week by Toronto Hydro after abnormal activity in its e-billing system was detected.

Toronto Hydro, after its initial review, believes that the personal information of some of its customers, including names, addresses, Hydro account numbers, the amount of the last bill and any money owed, may have been accessed.

Toronto Police have been called in by Toronto Hydro to investigate.

Letters about the breach have already been sent by Toronto Hydro to all of its customers. In that letter, the utility advised that any customer seeking more information can contact Toronto Hydro at 416-542-8000. The hours of Toronto Hydro's call-in centre have been extended, following a suggestion by Commissioner Cavoukian to do so.

The Information and Privacy Commissioner is appointed by and reports to the Ontario Legislative Assembly, and is independent of the government of the day. The Commissioner's mandate includes overseeing the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*, as well as the *Personal Health Information Protection Act*, which applies to both public and private sector health information custodians, in addition to educating the public about access and privacy issues.

Media Contact:

Bob Spence
Communications Co-ordinator
Direct line: 416-326-3939
Cell phone: 416-873-9746
Toll free: 1-800-387-0073
bob.spence@ipc.on.ca
www.ipc.on.ca

 2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

416-326-3333
1-800-387-0073
Fax/Tél.: 416-326-9195
TTY: 416-325-7539
<http://www.ipc.on.ca>



The Next Five Years ...
“Privacy by Design”



The Next Five Years

- “I will continue to emphasize the need to *embed privacy directly into IT*, at the earliest developmental stage.”
- “I will be working with all stakeholders in the health care field to help bring about *effective and privacy-protective electronic health record systems*.”
- “I will be strongly urging both provincial and local governments to be very *proactive in developing automatic disclosure programs* under which general records are routinely posted to government websites.”



www.smartprivacy.ca



Privacy by Design – “The sine qua non”

LAW - REGULATION & INDEPENDENT OVERSIGHT

EDUCATION & AWARENESS

ACCOUNTABILITY & TRANSPARENCY

SOCIETAL NORMS

MARKET FORCES

Data Security

Fair Information Practices

“SmartPrivacy is the umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protection to Smart Privacy Foundations, but one measure stands out as the sine qua non: *Privacy by Design*. Dr. Ann Cavoukian, Information & Privacy Commissioner of Ontario, Canada, August 13, 2009.

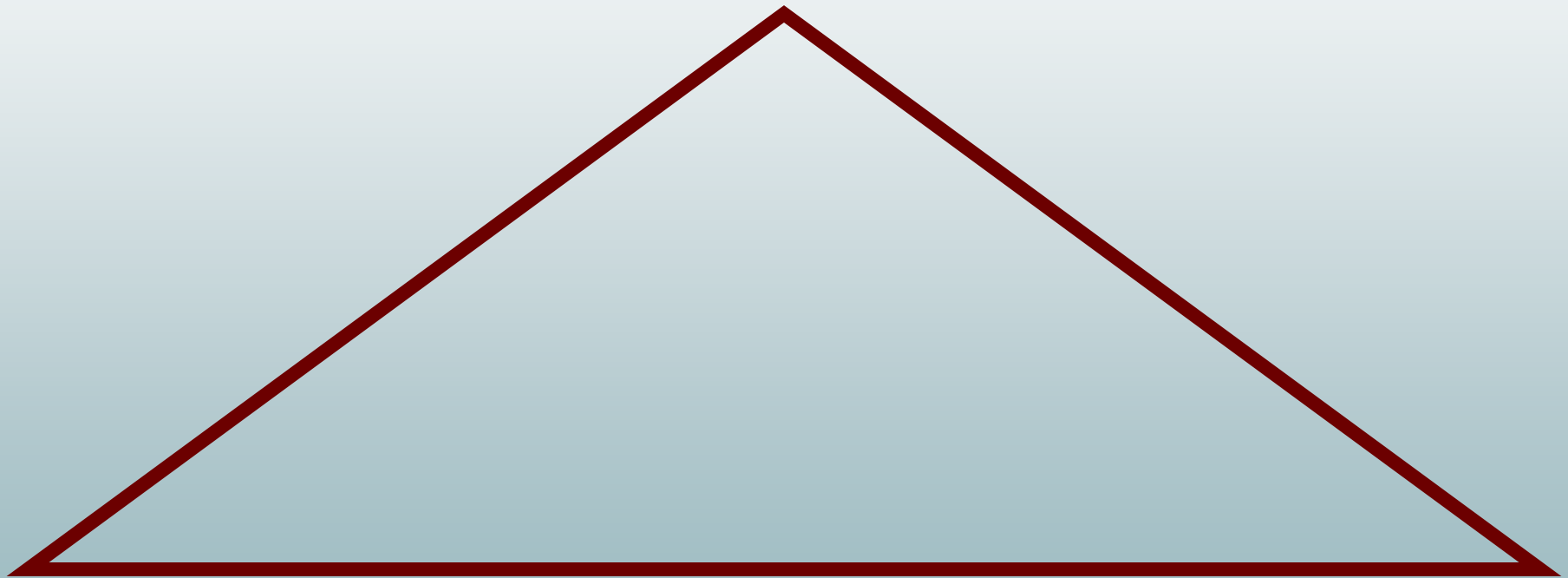


www.privacybydesign.ca



Privacy by Design: The Trilogy of Applications

Information Technology



**Accountable
Business Practices**

**Physical Design
& Infrastructure**



Privacy by Design: *Focus for 2009*

- **Technology** – Building privacy directly into technology, at the earliest developmental stage;
- **Accountable Business Practices** – Incorporating privacy into competitive business strategies and operations;
- **Physical Design and Infrastructure** – Ensuring privacy in health care settings and networked infrastructure.




Why We Need *Privacy by Design*

- Most privacy breaches remain undetected – as regulators, we only see the tip of the iceberg;
- The majority of privacy breaches remain unchallenged, unregulated, unknown;
- Compliance alone, is unsustainable as a model for ensuring the future of privacy; for that, we must turn to proactive measures such as *Privacy by Design*: embedding privacy proactively into the core of all that we do.



Privacy by Design: 7 Foundational Principles

1. *Proactive* not Reactive;
Preventative not Remedial
2. Privacy as the *Default*
3. Privacy *Embedded* into Design
4. Full Functionality: Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy


www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept that I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we understand that a more substantial approach is required – extending the use of PETs to taking a positive-sum, not a zero-sum, approach.

Privacy by Design now extends to a "Triology" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy protection requirements tend to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

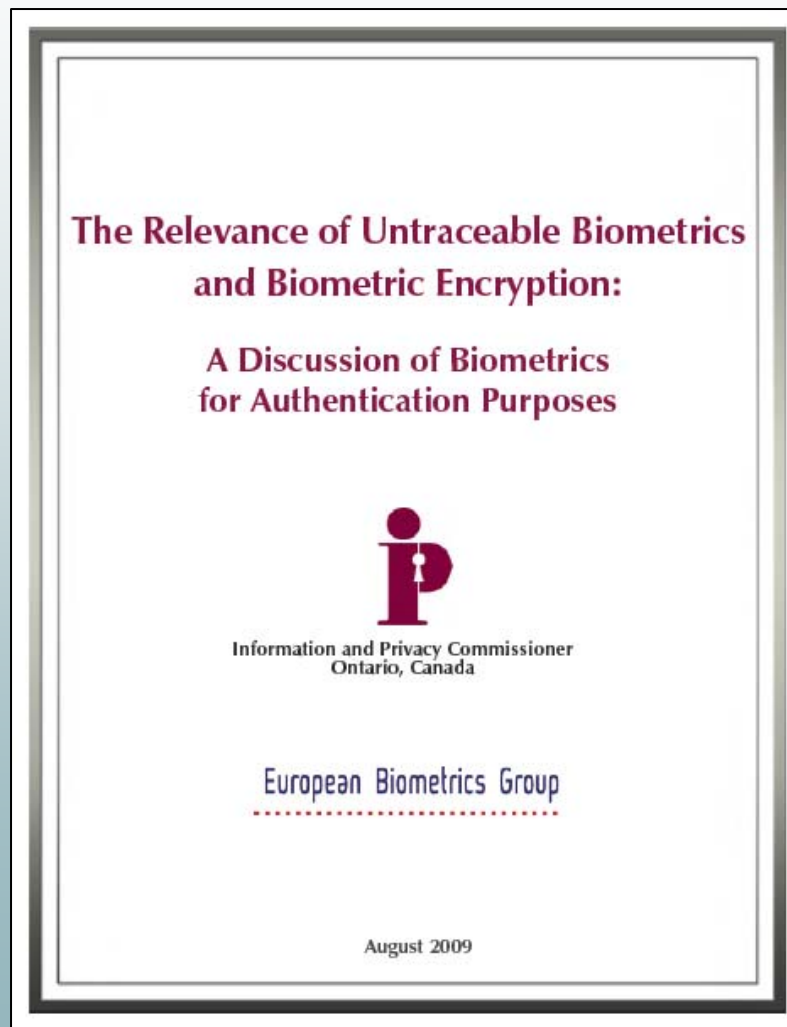
1. *Proactive* not Reactive; *Preventative* not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.



A Discussion of Biometrics for Authentication Purposes

- *Untraceable Biometrics*
— Ann Cavoukian, Ph.D.;
- *Anonymous Biometrics*
— Max Snijder.

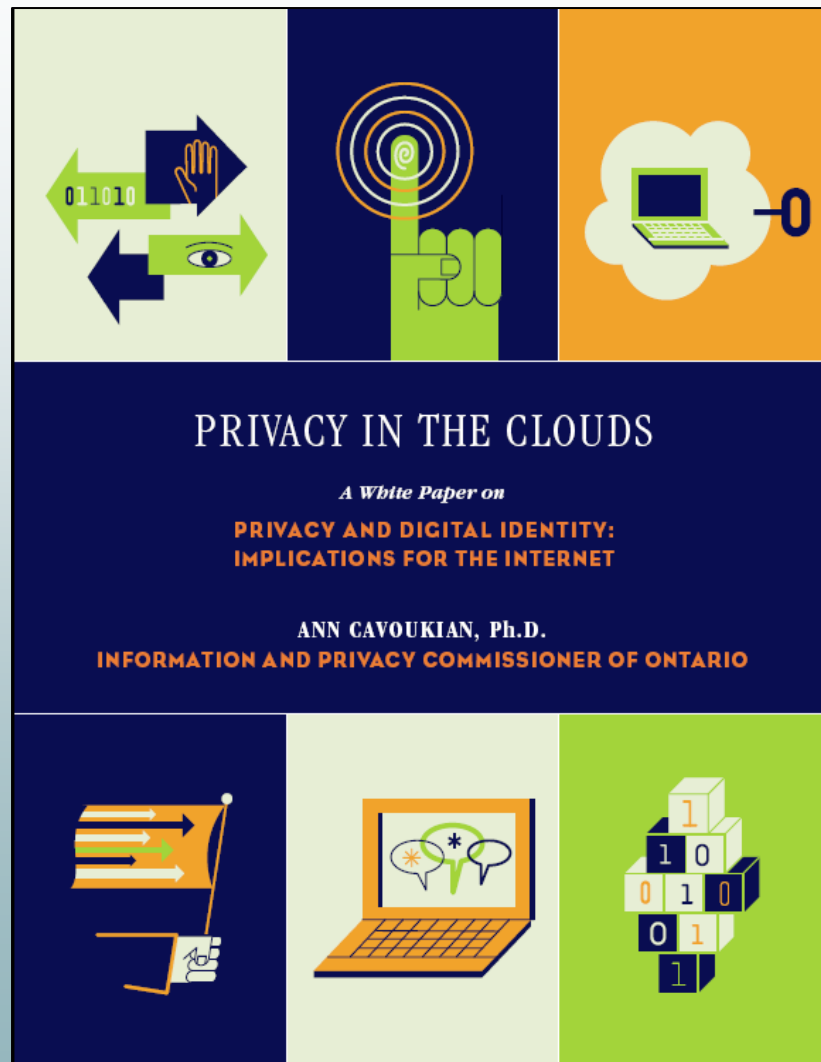




Privacy in the Clouds

A White Paper on Privacy and Digital Identity: Implications for the Internet

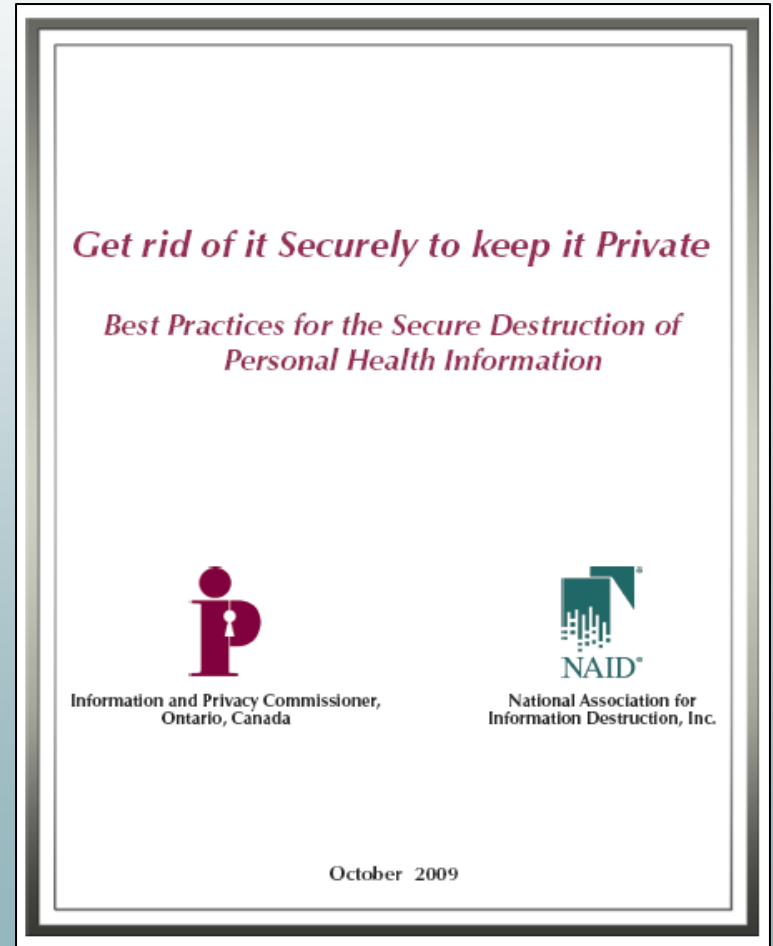
- The 21st Century Privacy Challenge;
- Creating a User-Centric Identity Management Infrastructure;
- Technology Building Blocks;
- A Call to Action.





Get Rid of it Securely to Keep it Private – Best Practices for the Secure Destruction of Personal Health Information

1. Develop and implement a secure destruction policy;
2. Segregate and securely store personal health information;
3. Determine best methods of destruction;
4. Document the destruction process;
5. Considerations prior to employing a service provider;
6. Disposal of securely destroyed materials;
7. Auditing and ensuring compliance.





Smart Grid and Ontario's Smart Meter Initiative

- The Government of Ontario has committed to install a smart electricity meter in all homes and small businesses by the end of 2010 – *Energy Conservation Responsibility Act, 2006*;
- Smart meters will record electricity consumption on an hourly basis and report that information via a wireless technology;
- Individuals will be able to access their meter data from the previous day and be able to make choices about how to take advantage of future rates;
- A 'smart metering entity' (the Independent Electricity System Operator, or IESO) will receive and process the hourly consumer consumption data transmitted daily;
- The IESO is a listed institution under Ontario's *FIPPA*.



RFID Transformed: The Problem

- WHTI-compliant passcards and Enhanced Driver Licences (EDLs) contain passive RFID tags;
- These ID cards are being rolled out in border states and provinces, including Ontario;
- Our position: you should be able to turn the RFID off – the *default should be off* (the most privacy-protective option), unless the user chooses to turn it *on*, when needed.



RFID Transformed: The Solution

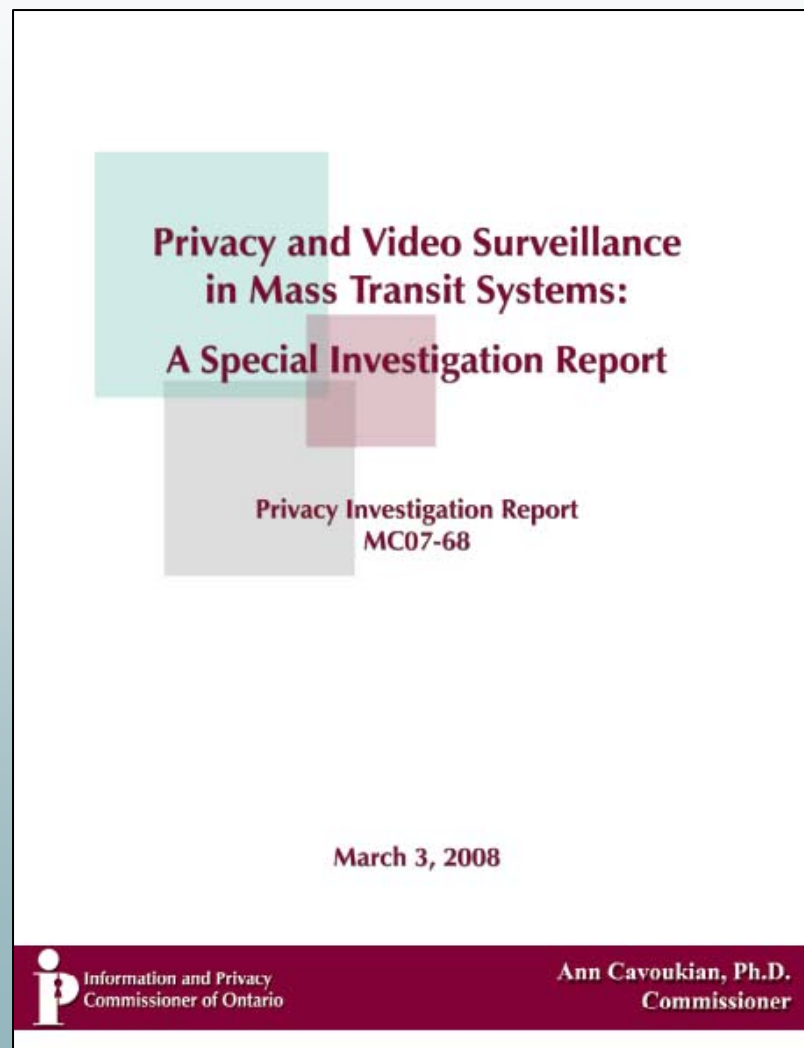
- We asked technology experts, *how can you turn it off?*
- Impinj® Inc., (www.impinj.com), has developed a prototype Gen2 RFID Tag (TouchTag™) that functions only when activated by human touch – at a distance of up to 30 feet (9 metres);
- The tag remains *inoperative* (off) until the user touches a specific spot on the tag, which then enables the tag to be read;
- When the user releases his or her finger from the tag, it once again becomes inoperative – it turns off (which becomes the default);
- * • **November 2, 2009** – Impinj® Inc. will be joining me in Madrid at the *Privacy by Design Workshop* where they will also have their RFID Tag technology on display – www.privacybydesign.ca/madrid09.htm



Toronto Transit Commission

Surveillance Cameras

- In March 2008, I ruled that Toronto's Mass Transit System's use of video surveillance cameras was in compliance with Ontario's privacy law.
- However, I called upon the TTC to undertake a number of specific measures to enhance privacy:
 - Personal information will only be collected for legitimate, limited and specific purposes;
 - Collection will be limited to the minimum necessary and **only retained up to 72 hours;**
 - A comprehensive audit of the video surveillance system must be conducted by an independent third party using the GAPP (Generally Accepted Privacy Principles).





CCTV Cameras:

Innovative Privacy-Enhancing Approach to Video Surveillance

- At the University of Toronto, Professor Kostas Plataniotis and Karl Martin have developed a privacy-enhancing approach to video surveillance cameras;
- Their work, as described in *Privacy Protected Surveillance Using Secure Visual Object Coding*, uses cryptographic techniques to secure a private object (a face/image), so that it may only be viewed by designated persons;
- Objects of interest (e.g. a face or body) are stored as completely separate entities from the background surveillance frame, and strongly encrypted;
- **Xiris Automation Inc.** and the **MaRS Centre** are currently working on commercializing this technology.



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