

Changing the Paradigm: *Privacy by Design*

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario**

**Ryerson University
Law and Business Students' Association
*November 17, 2009***



Presentation Outline

- 1. We Need to Change the Paradigm,
... SmartPrivacy and Privacy by Design*
- 2. The Next Wave: From PETs to PETs Plus,
... to Transformative Technologies*
- 3. Biometrics Transformed: Biometric Encryption*
- 4. Video Surveillance Transformed*
- 5. RFID Transformed: Add an On/Off Switch*
- 6. SmartPrivacy for the Smart Grid*
- 7. Conclusions*



*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 mutually 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, or privacy *and* functionality, 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
and false dichotomies*



Why We Need Technology to Protect Privacy

“We need technology ... citizens need technology to protect themselves because the law is *not* doing it.”

— Jennifer Granick

Electronic Frontier Foundation

SmartPrivacy

www.smartprivacy.ca



Privacy by Design – “The sine qua non”

LAW - REGULATION & INDEPENDENT OVERSIGHT

EDUCATION & AWARENESS

ACCOUNTABILITY & TRANSPARENCY

AUDIT & CONTROL

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



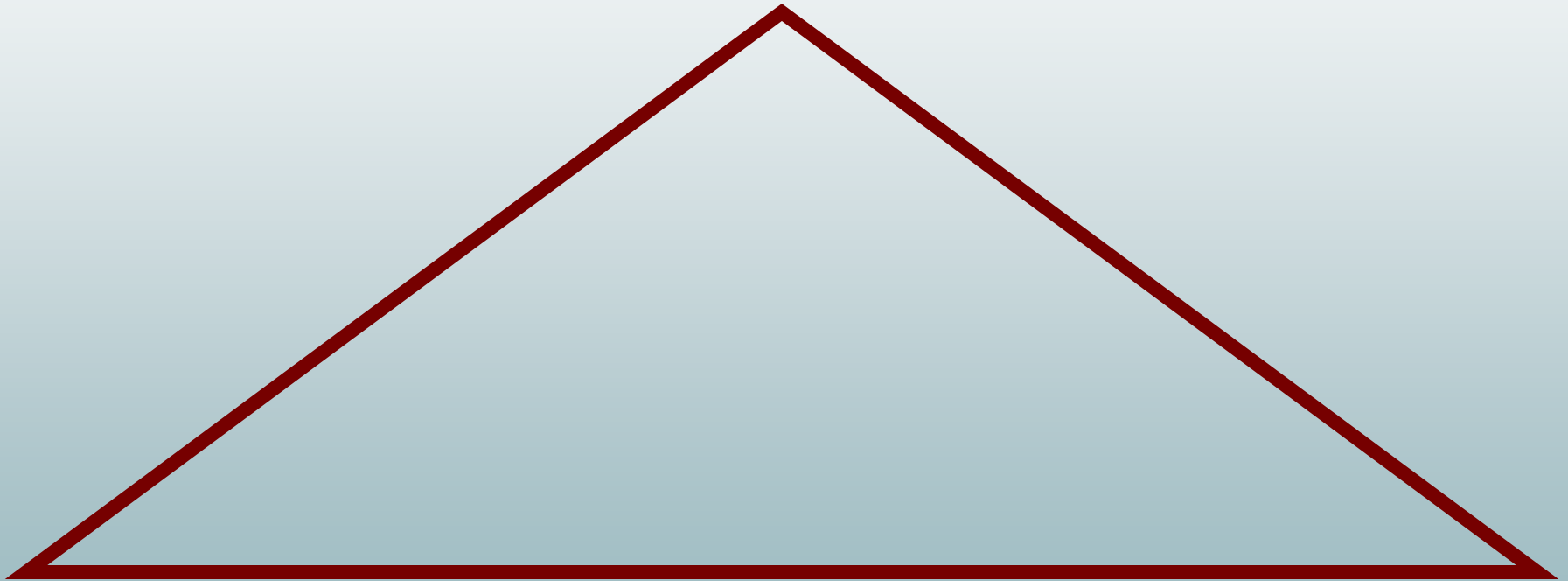
Privacy by Design: “Build It In”

- I first developed the concept of “Privacy by Design” in the 90s, 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 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*

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: **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



Privacy by Design: The 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.



The Next Wave:

From PETs to PETs Plus,

to

Trans Tech



Background:

Privacy-Enhancing Technologies (*PETs*)

- The IPC and the Dutch Data Protection Authority advanced the concept and methodology recognized around the world today as *privacy-enhancing technologies* (PETs);
- In 1995, the IPC and the Dutch Data Protection Authority published their landmark study, *Privacy-Enhancing Technologies: The Path to Anonymity*.

Vol. I - www.ipc.on.ca/index.asp?layid=86&fid1=329

Vol. II - www.ipc.on.ca/images/Resources/anoni-v2.pdf



Time for a Change...

***... from PETs
to
PETs Plus***



PETs *Plus*

The “*Plus*” in PETs *Plus* refers to incorporating a positive-sum (not-zero-sum) paradigm



Taking PETs *Plus* Further

from PETs Plus

to ...

Transformative Technologies



Transformative Technologies

**Privacy-Invasive Technology + Positive-Sum Paradigm +
Privacy-Enhancing Technology =
Transformative Technology**

Common characteristics of Transformative Technologies:

- Minimize the unnecessary collection, disclosure, use and retention of personal data;
- Empower individuals to participate in the management of their own personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in personal data governance structures;
- Promote/facilitate the commercialization and adoption of these technologies.



Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum

- Examples of Transformative Techs if *PbD* enabled:
 - Biometric Encryption
 - Video Surveillance
 - RFID

**Transformative Technologies Deliver
Both Security and Privacy:
Think Positive-Sum not Zero-Sum**

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

Privacy, in the form of informational privacy, refers to an individual's ability to exercise personal control over the collection, use and disclosure of one's recorded information. Thus far, a "zero-sum" approach has prevailed over the relationship between surveillance technologies and privacy. A zero-sum paradigm describes a concept or situation in which one party's gains are balanced by another party's losses – win/lose. In a zero-sum paradigm, enhancing surveillance and security would necessarily come at the expense of privacy; conversely, adding user privacy controls would be viewed as detracting from system performance. I am deeply opposed to this viewpoint – that privacy must be viewed as an obstacle to achieving other technical objectives. Similarly, it is unacceptable for the privacy community to reject all forms of technology possessing any surveillance capacity and overlook their growing applications.

Rather than adopting a zero-sum approach, I believe that a "positive-sum" paradigm is both desirable and achievable, whereby adding privacy measures to surveillance systems need not weaken security or functionality but rather, could in fact enhance the overall design. A positive-sum (win-win) paradigm describes a situation in which participants may all gain or lose together, depending on the choices made.

To achieve a positive-sum model, privacy must be proactively built into the system (I have called this "privacy by design"), so that privacy protections are engineered directly into the technology, right from the outset. The effect is to minimize the unnecessary collection and uses of personal data by the system, strengthen data security, and empower individuals to exercise greater control over their own information. The result would be a technology that achieves strong security *and* privacy, with a "win-win" outcome.

By adopting a positive-sum paradigm and applying a privacy-enhancing technology to a surveillance technology, you develop, what I am now calling, "Transformative Technologies." Among other things, transformative technologies can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive, serving to minimize the unnecessary collection, use and disclosure of personal data, and promoting public confidence and trust in data governance structures.

**Positive-Sum Paradigm + Privacy-Enhancing Technology
(applied to Surveillance Technology) = Transformative Technology**



Biometrics Transformed: Biometric Encryption



IPC and Biometrics

- The IPC has been a longstanding proponent of biometric encryption technologies;
- We continue to press for strong privacy protections in the development and deployment of interoperable biometric technologies;
- Active member of the European Biometrics Forum International Biometrics Advisory Council (IBAC).

www.eubiometricforum.com/index.php?option=content&task=view&id=457



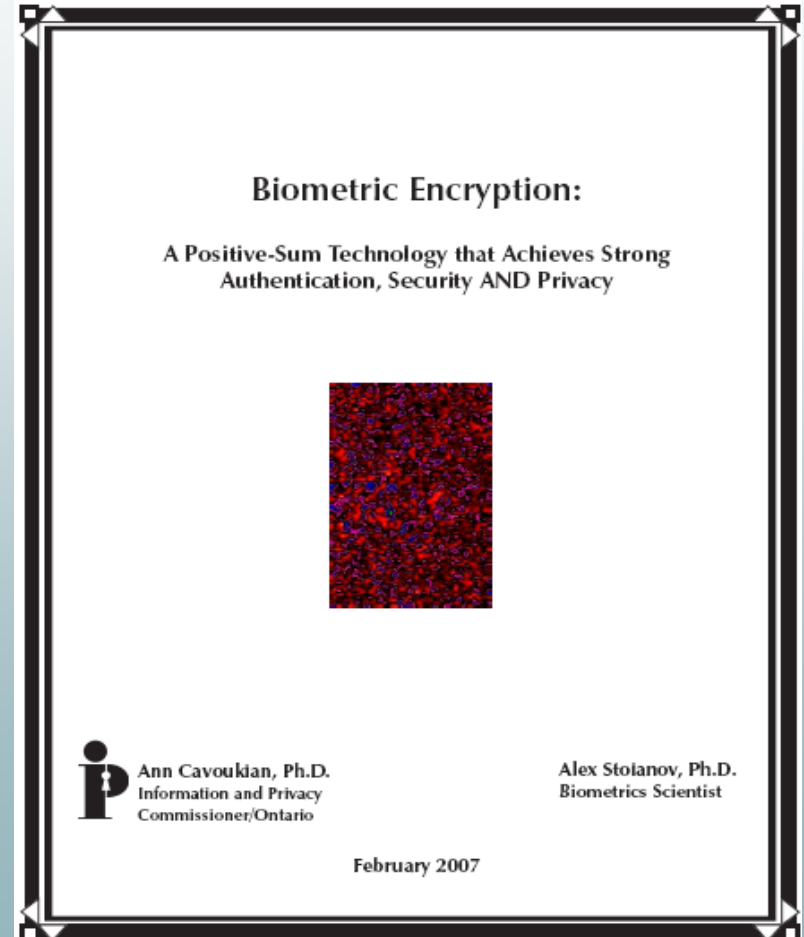
European Biometrics Forum

- The European Biometrics Forum (EBF) was launched in 2003; Member of International Biometrics Advisory Council (IBAC);
- Composed of leading biometrics and technology experts, the EBF was established to develop world-class standards, best practices and innovation in the biometrics industry to strengthen trust and confidence in the use of emerging biometric applications;
- The EBF is supported by a network of national biometric organizations, companies, universities and experts across Europe in carrying out research for the development of a roadmap for the European Biometrics industry to 2010.



Biometric Encryption: *A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*

- Privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of BE over other uses of biometrics;
- How BE technology can help to overcome the prevailing “zero-sum” mentality by effectively transforming one’s biometric to a private key.





Biometric Encryption (BE)*

What is Biometric Encryption?

- Class of emerging “untraceable biometric” technologies that seek to transform the biometric data provided by the user;
- Special properties:
 - uniqueness
 - irreversibility

* Pioneering development by George Tomko, Ph.D.
Founder of Mytec Technologies, 1994.



Biometric Encryption

- Biometric encryption is a process that securely binds a PIN or a cryptographic key with a biometric, so that neither the key nor the biometric can be retrieved. The key is recreated only if the correct live biometric sample (a finger or iris) is presented on verification;
- In biometric encryption, you can use the biometric to encrypt a PIN or a password for numerous applications, such as access to computers or bank machines. The PIN can be 100s of digits in length since you don't need to remember it;
- Most important, the only item that has to be stored in a database is the biometrically encrypted PIN or password, not the biometric template, so privacy is preserved.



Current BE Projects

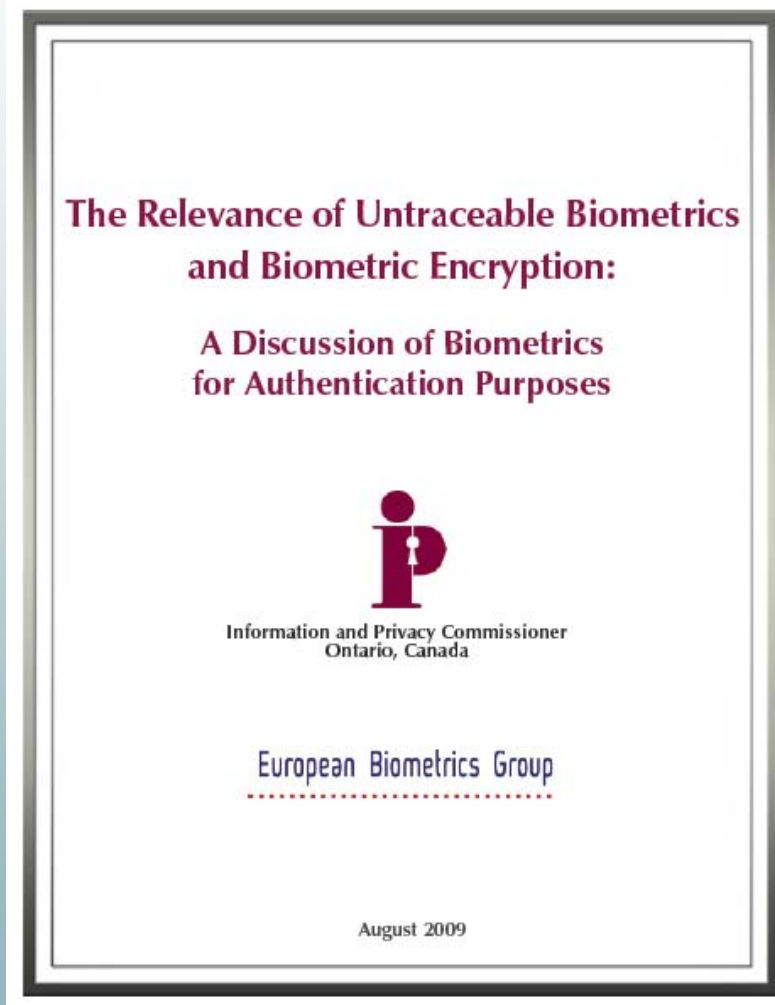
- **The Philips privID™ (Netherlands)** – is currently one of the most advanced BE technologies in operation; unlike some BE systems, the privID™ system is very fast which allows for a true one-to-many mode; it is also very secure, making it extremely difficult to crack;
- **PerSay (Israel)** – has successfully combined their own voice authentication technology with Philips' BE technology making voice biometric encryption a reality;
- **Ontario Lottery and Gaming (OLG)** – Professor Kostas Plataniotis and Karl Martin, University of Toronto, have developed a privacy-enhancing approach to video surveillance cameras using cryptographic techniques so that it may only be viewed by unlocking the encrypted object with a secret key. The OLG is now exploring the possibility of using this technology for their self-exclusion program.



A Discussion of Biometrics for Authentication Purposes

- *Untraceable Biometrics*
— Ann Cavoukian, Ph.D.;
- *Anonymous Biometrics*
— Max Snijder.
- *Encyclopaedia of Biometrics:
Encryption, Biometric*
— Ann Cavoukian, Ph.D. &
Alex Stoianov, Ph.D.

www.springer.com



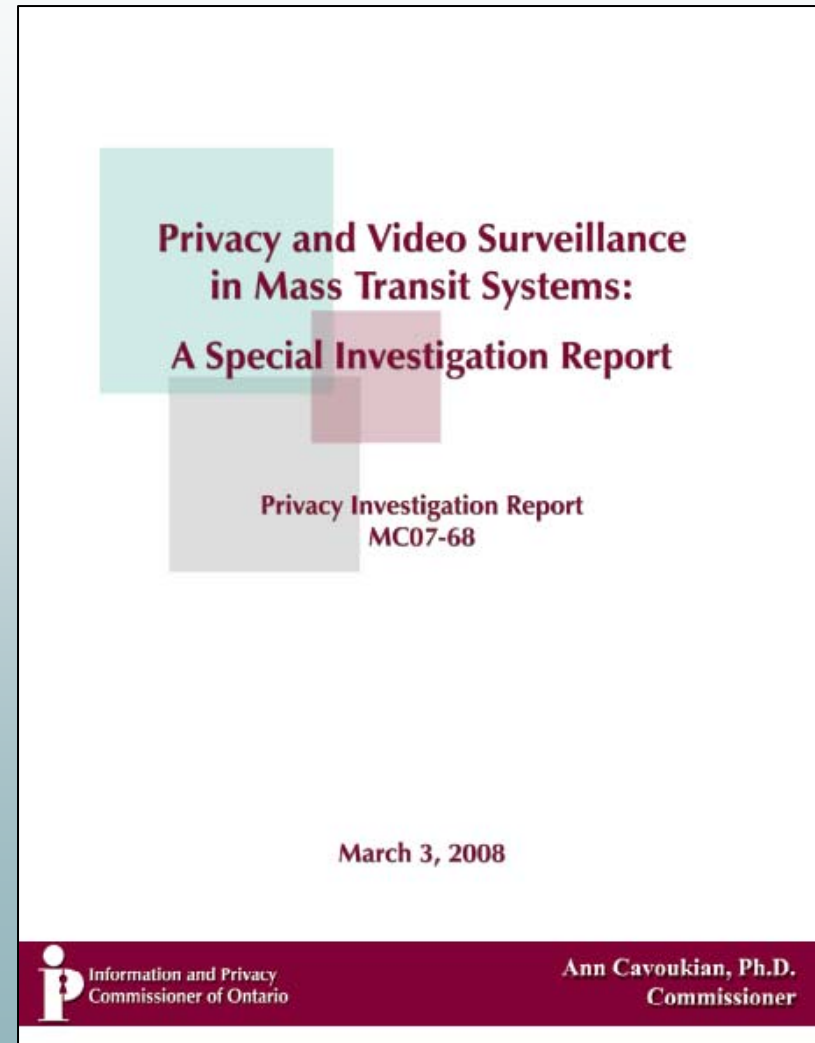


Video Surveillance Transformed



TTC 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).





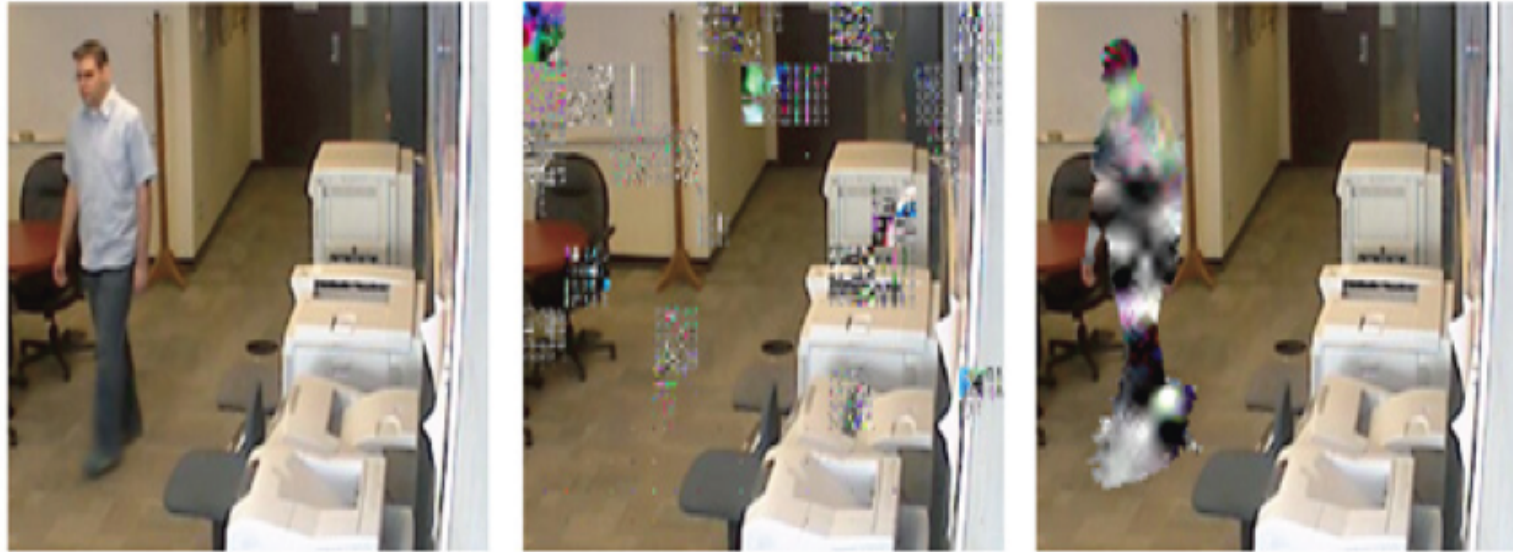
CCTV Cameras:

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.



Innovative Privacy-Enhancing “Transformative” Approach



(a)

(b)

(c)

Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and despite attempts to hack into this with an incorrect key, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.



TTC Report: What the Experts are Saying

“The report is a valuable step forward toward ensuring that video surveillance be carried out in ways that ensure that privacy is protected and that oversight exists.”

— Professor Daniel J. Solove, Associate Professor of Law,
George Washington University Law School

“While I understand your report is specifically addressing only the Toronto Transit Commission, it will be invaluable to municipalities throughout the world which are facing similar vexing questions about the proper use and management of video surveillance technologies. Your recommendations provide a principled yet workable model for how to protect individuals' legal and moral right to privacy while also advancing the public's interest in safe, efficient and affordable infrastructure.”

— Professor Fred Cate, Distinguished Professor of Law and
Director, Center for Applied Cybersecurity Research



TTC Report: What the Experts are Saying (Cont'd)

“It sets the bench mark for informed discussion of CCTV in mass transit systems ... It provides a roadmap for the most privacy protective approach to CCTV. It offers potential technological solutions that can further enhance privacy with CCTV imagery. It presents specific recommendations and a requirement for an independent third-party audit (this is the Commissioner flexing her muscles). Finally, it demonstrates that ... good system design, vigilant oversight, and a commitment to privacy values can result in ‘positive-sum’ models as Commissioner Cavoukian describes them.”

— Murray Long, Editor and Publisher,
PrivacyScan



EPIC Book Review:

Privacy by Design ... Take the Challenge

“Dr. Cavoukian's work over the last twenty years has been a steady evolution of ideas. In 1995, she promoted Privacy-Enhancing Technologies (PETs) with the Netherlands Data Protection Authority. This term has been instrumental in guaranteeing the continued presence of privacy protections by building them into technology.”

*— EPIC Book Review,
November 9, 2009.*



EPIC Alert (16.21) Book Review – November 9, 2009:

**“Privacy By Design . . . Take the Challenge”
by Ann Cavoukian, Ph.D.**

Available at: <http://www.ipc.on.ca>

Ann Cavoukian is a rare breed — a government official working with privacy and technology who genuinely seems to understand both. In Privacy By Design, the current Information and Privacy Commissioner of Ontario Canada proves it. Dr. Cavoukian's recent work compiles a number of reports, guidelines, speeches, and essays published by her and her office in recent years. These various pieces combine to show a comprehensive approach to privacy in a modern world.

Dr. Cavoukian's work over the last twenty years has been a steady evolution of ideas. In 1995, she promoted Privacy-Enhancing Technologies (PETs) with the Netherlands Data Protection Authority. This term has been instrumental in guaranteeing the continued presence of privacy protections by building them into technology. Later in the decade, she argued for the concept of “privacy by design,” a philosophy in which privacy is embedded into the technology itself during development, such that privacy and data protection become part of designers' original goals. While this view has become more prominent, Dr. Cavoukian was instrumental in its adoption.

In her current work, Dr. Cavoukian expands her idea of PETs into a new concept, which she calls “PETs Plus.” This concept is the idea that privacy need not be part of a zero-sum model, in which increasing privacy comes at a cost to efficacy. Instead, Cavoukian argues for a positive-sum model, in which privacy can be increased alongside security, or alongside business practices, so that focusing on data protection has only net benefits for designers and implementers of technology.

Many of the essays in Privacy by Design include examples of these PETs Plus, and many of them are quite impressive. In her discussion of CCTV, Dr. Cavoukian describes a new development in which people's images in the video stream are encrypted. This allows a person to monitor the video live for suspicious behavior without ever seeing anyone's identity. If the video contains evidence of a crime, proper law enforcement officials can decrypt that section, with a suitable audit trail ensuring that only the necessary information is decrypted.

Another excellent PET Plus is a design from IBM for radio frequency identification (RFID) tags that can be disabled or even reprogrammed by the consumer, which would allow the tags to be useful in inventory and sales management, while giving individuals the ability to decide exactly how they will be used at home. Dr. Cavoukian also discusses an advanced method for securing and encrypting biometric authentication systems, and privacy-maximizing best practices for a number of security processes, including CCTV, RFID in healthcare, and airport searches. Privacy By Design is a must-read for anyone in the security or privacy fields looking for the best approach to new technology.

— Jared Kaprove





Toronto Police Services

Surveillance Cameras

- The Toronto Police Service (TPS) conducted a pilot project to test Closed Circuit Television (CCTV) video surveillance in specific high-crime areas, as an added tool for the detection and deterrence of crime and enhancing public safety and security;
- Members of the TPS met with the IPC to apprise us of this proposal. The Police were aware of the IPC's *Guidelines for Using Video Surveillance Cameras in Public Places* and stated their intention to adhere to them;
- IPC personnel conducted a site visit at the outset of the pilot project, and the TPS kept the IPC informed of developments during the program, which concluded with an evaluation in Spring 2008.



Toronto Police Services

Support for Positive-Sum Approach

“This governance model has ensured a **positive-sum approach** to the use of public space cameras in Toronto, one that enables the use of this additional tool to support policing while concurrently mitigating privacy concerns through technological and operational design.”

— Chief of Toronto Police Services, William Blair,
October 22, 2009.



***RFID, Transformed:
Add an
On/Off Device***



RFID, Transformed: The Problem

- Privacy concerns arise when RFIDs are *associated with personally identifiable individuals*;
- Without appropriate security measures, embedding passive RFIDs into identity cards is problematic;
- The solution generally proposed – a protective sleeve, or Faraday Cage, is not sufficient.



The Problem (Cont'd)

- 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?*
- This will have profound implications for use in RFID-enabled payment and access cards, and other forms of identification;
- 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).



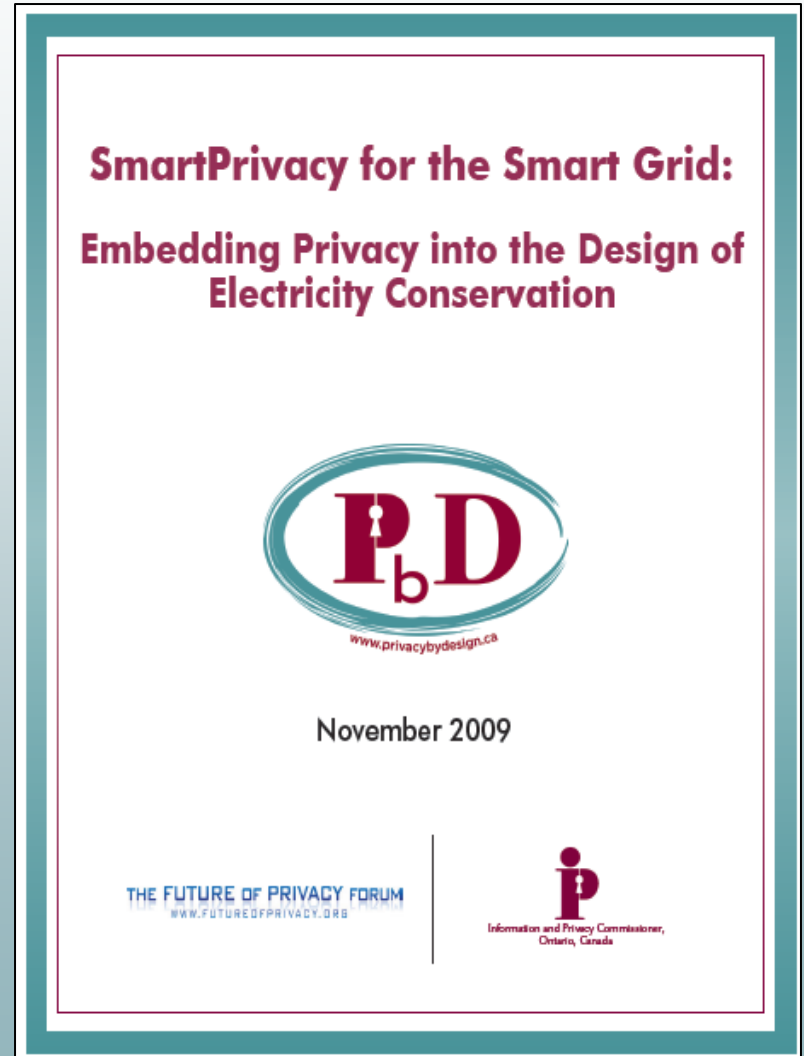
*SmartPrivacy for the
Smart Grid*



SmartPrivacy for the Smart Grid

- Released today, with the Future of Privacy Forum.

www.privacybydesign.ca





Smart Grid:

What is It?

- “Smart Grid” refers to the modernization of the current electrical grid so that there is bi-directional flow of information and electricity in order to achieve the following goals:
 - provide consumers with more choices on how, when, and how much electricity they use;
 - self-heal in case of disturbances, attacks, and natural disasters;
 - link with a wide array of energy sources, in addition to energy produced by power plants, such as renewable energy producers;
 - provide better power quality, and more efficient delivery of electricity;
- Communications technology and infrastructure is at the heart of improvements to the electrical grid, which will collate data provided by smart meters, sensors, and computer systems into understandable and actionable information.



Smart Grid: *Privacy Risks*

- Modernization of the current electrical grid will involve end-user components and activities that will tend to increase the collection, use and disclosure of personal information by utility providers, as well as perhaps third-parties;
- In the context of the Smart Grid, the linkage of any personally identifiable information with energy use would render the linked data as personal information;
- The information collected on a smart grid can also form a library of personal information, the mishandling of which can lead to invasion of consumer privacy;
- An electricity usage profile can translate into a source of detailed behavioural information;
- Major concerns will arise if consumer-focused principles of transparency and control are not treated as essential design principles, from end to end.



SmartPrivacy for the Smart Grid

Smart Grid	Smart Grid + <i>SmartPrivacy</i>
<p>Intelligent – capable of sensing system overloads and rerouting power to prevent or minimize a potential outage; of working autonomously when conditions require resolution faster than humans can respond...and cooperatively in aligning the goals of utilities, consumers and regulators.</p>	<p>Intelligent – capable of collecting the minimum amount of personal information necessary from consumers, without diminishing the quality and range of services offered. Works transparently with consumers to communicate information regarding the collection, use and disclosure of their personal information. Plans in advance how to protect Privacy and security has been built into the system in advance of its use.</p>
<p>Efficient – capable of meeting increased consumer demand without adding infrastructure.</p>	<p>Efficient – capable of meeting increased consumer demand without compromising the privacy and security of personal information. Securely disposes of personal information when it is no longer needed for the purpose for which it was originally collected.</p>
<p>Accommodating – accepting energy from virtually any fuel source including solar and wind as easily and transparently as coal and natural gas; capable of integrating any and all better ideas and technologies – energy storage technologies, for example – as they are market-proven and ready to come online.</p>	<p>Accommodating – accepting of a variety of consumer preferences with regards to the use, retention, and disclosure of personal information - makes these options easily accessible to the individual.</p>



SmartPrivacy for the Smart Grid

(Cont'd)

Smart Grid	Smart Grid + <i>SmartPrivacy</i>
<p>Motivating – enabling real-time communication between the consumer and utility so consumers can tailor their energy consumption based on individual preferences, like price and/or environmental concerns.</p>	<p>Motivating – enabling communication and notice between the consumer and utility so that consumers can tailor their personal information options, based on individual preferences. Proactively obtains positive consent <i>before</i> disclosing any personal information to a third party.</p>
<p>Opportunistic – creating new opportunities and markets by means of its ability to capitalize on plug-and-play innovation wherever and whenever appropriate.</p>	<p>Opportunistic – creating new opportunities and markets by means of its ability to capitalize on privacy-enhancing technologies, wherever and whenever appropriate.</p>
<p>Quality-focused – capable of delivering the power quality necessary – free of sags, spikes, disturbances and interruptions – to power our increasingly digital economy;</p>	<p>Quality-focused – capable of delivering information that is free of inaccuracies, and allowing individuals to access to their personal information and make any corrections necessary.</p>
<p>Resilient – increasingly resistant to attack and natural disasters as it becomes more decentralized and reinforced with Smart Grid security protocols.</p>	<p>Resilient – increasingly resistant to data leakage and breaches of personal information - reinforced with privacy and security protocols, such as privacy by default and breach notification.</p>
<p>“Green” – slowing the advance of global climate change And offering a genuine path toward environmental improvement.</p>	<p>“Green” – ensuring consumer trust in the Smart Grid, fostering greater participation by individuals leading to Environmental improvement.</p>



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*.



Smart Grid:

Where the IPC stands

- While the smart grid is a good idea, the focus has almost exclusively been on controlling energy use, making privacy a sleeper issue. We must take care not to sacrifice consumer privacy amidst a sea of enthusiasm for electricity reform;
- Principles of *Privacy by Design* must be part of the overall design for smart grid data flows;
- Fortunately, in Ontario, the ‘smart metering entity’ is subject to the *Freedom of Information and Protection of Privacy Act* (FIPPA).

*Online
Social Networks*



Our Work with Facebook

- In 2005, we were first approached by senior executives from Facebook seeking input on their privacy measures;
- This work included holding a student focus group to determine if and how students are aware of their privacy options;
- From our interaction with these students, we made the surprising discovery that none of them had set their privacy filters, and most were completely unaware of the privacy options available to them;
- We felt it was critical to get the message out that while social networking websites can be addictive, they can also be dangerous;
- We wanted these students and others to understand that when they choose to connect with their friends through a social networking website, they must remember that it is they who are ultimately responsible for determining what information they share with others.



Conference on Youth Privacy

- Last year, the IPC held a conference *Youth Privacy Online: Take Control, Make It Your Choice!* – attended by professionals from a diverse range of public and private sector organizations including education, technology and social studies.
- The conference also highlighted the work of my office in developing and distributing educational materials to schools. To date, we have distributed:
 - **8,500** copies of our brochure – *When Online Gets Out of Line: Privacy - Make an Informed Online Choice*
 - **7,000** copies of our Tip Sheet – *How to Protect Your Privacy on Facebook*
 - **500** copies of our brochure – *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*
 - **500** copies of our DVD – *Be A Player: Take Control of Your Privacy on Facebook*
- We have also recently updated our IPC School-Kits to include material on how to safely navigate and engage in online social activities.



Youth Privacy Online:

Take **Control**

Make it **your choice!**



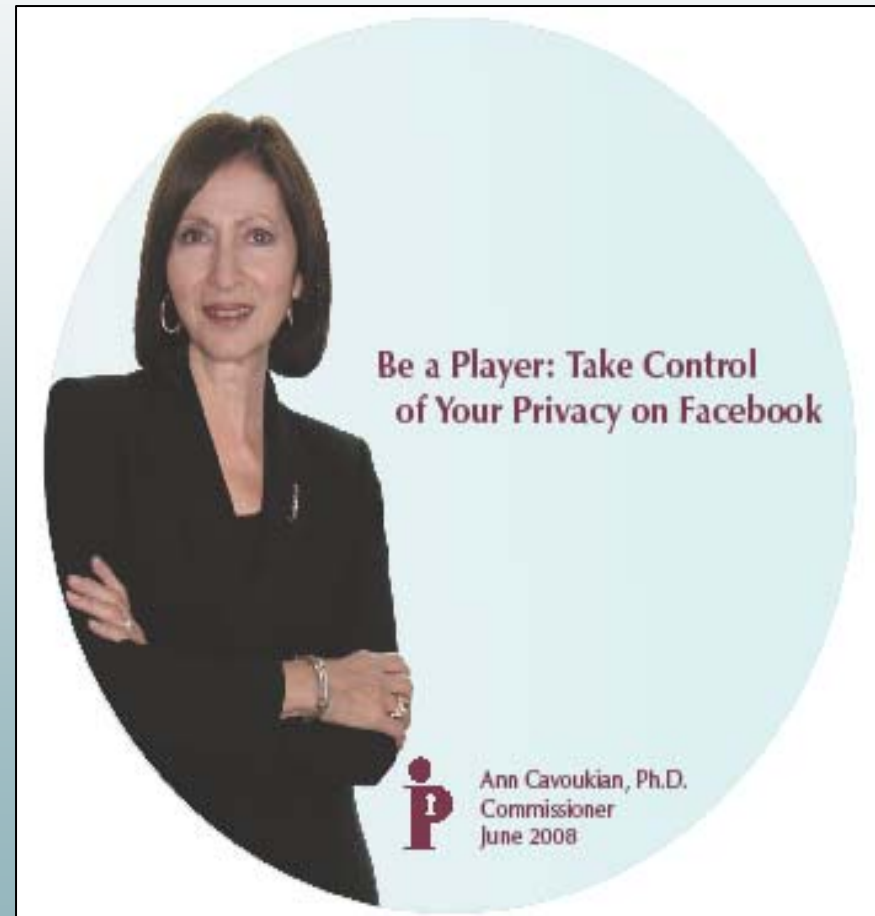
September 4, 2008  Eaton Centre Marriott  **Be there!**



Joint IPC-Facebook Video:

Be a Player: Take Control of Your Privacy on Facebook

- Issues covered in our video include weak privacy controls, the intrinsic risks involved in using them, and some of the protections students should be aware of when posting their personal information online, such as being able to control access to one's profile and being able to block access to specific information.
- This video can be viewed at www.ipc.on.ca or for a free copy, please email our office at publicat@ipc.on.ca.





IPC Brochure: *When Online Gets Out of Line*

- University and high school students need to consider all the potential implications before posting personal information to online social networking sites;
- It is important that students take the time to make informed choices about the site they use, the information they post and those with whom they choose to share their information;
- Going on “automatic pilot” online is a bad idea. *Always think before you click!*






IPC Facebook Tipsheet

How to Protect Your Privacy on Facebook

- When you sign up as a user of Facebook, the default settings allow all other Facebook users to find you in searches;
- By default, your name and thumbnail profile picture can also be found on public search engines. Facebook has selected these settings based on what it believes most users want, but you can always change them to restrict access to your information, as you see fit.



How to Protect your Privacy on Facebook

When you sign up as a user of Facebook, the default settings allow all other Facebook users to find you in searches. However, only those you have confirmed as friends or who share a network with you have access to your full profile. By default, your name and thumbnail profile picture can also be found on public search engines. Facebook has selected these settings based on what it believes most users want, but you can always change them to restrict access to your information, as you see fit. Therefore, you can change the default settings to restrict access to your profile. Under the current setting, only your friends, their friends and the people on your networks can see your profile. If you download Facebook Platform third-party applications into your profile, some of your information may be shared (see section on Applications below). It is important to explore these default settings, to adjust the privacy settings to that with which you are comfortable.

It's easy to change the default settings. Once you sign in, click on "privacy" on the top-right side of the screen or the bottom-right side, or visit <http://Facebook.com/privacy>. The Privacy Overview menu has four categories in which you can determine the degree of privacy you would like. You can click on each heading to access the page on which you can make your changes. Privacy settings can be customized to exclude or include specific friends or lists of friends. Creating these lists is done in the Friends section of the site by clicking on the Make a New List button and following the step-by-step instructions.

Profile: This page contains two tabs, each with numerous individual controls for who can see aspects of your profile. On the Basic tab are controls for your entire profile, and individual features of your profile: Basic Information (which includes Gender, Birthday, Hometown, Political and Religious Views, and Relationship Status), Personal Information (which includes your Interests, Activities, Favorites and your About Me section), photos and videos tagged of you, status updates, online status, friends, wall, education and work information. On the Contact Information tab, you can tailor permissions for IM Screen Name, Mobile Phone, Land Phone, Current Address, Website and Email Address (if in fact you provided these details for your profile).

- To limit viewing of Profile information to only your Facebook friends, select "All Friends" in each drop-down menu. If you wish to limit viewing to certain segregated lists of friends that you can set up on your main Friends page, or just to individual friends, or to exclude certain individuals and networks, choose "Customize" in the drop-down menus and adjust the settings accordingly.

Search: You can control which Facebook users can find you in searches and what appears in your search listing within the site; more importantly, you can control whether you are searchable by anyone on public search engines. Within Facebook, you can restrict which networks have access to your profile in searches and what actions people can take with your search results, such as contacting you or adding you as a friend.

- To be searchable only by your Facebook friends, select "All Friends" in the Search Visibility drop-down menu and leave the first set of checkboxes below the drop-down menu blank.
- To avoid being searchable on public search engines, when you have selected "Everyone" in the drop-down menu simply uncheck the box next to "Create a public search listing for me."

News Feed and Mini-Feed: This page has three tabs. On the "Actions Within Facebook" tab, you can control what actions show up automatically in your Mini-Feed and your friends' News Feeds.

- "Uncheck" any actions that you do not want your friends to know about automatically, such as when you make a comment on a posted item or add a friend.

On the "Actions on External Websites" tab, you can opt out of having your activity on external websites of certain partner organizations posted to your Facebook profile's Mini-Feed, where it may also appear on your friends' News Feeds. This is a feature known as Facebook Beacon; there are numerous partner websites including Epicurious, Typepad, Blockbuster, etc.



Talking to Youth: Beware of *the 5 Ps*

- I have spoken at a number of schools in my attempt to reach out to students regarding how they can stay safe, and in control, while online. My main message to them has been to always be aware of the 5 Ps:

1. Predators

2. Parents

3. Professors (Teachers)

4. Prospective employers

5. Police



Conclusions

- Lead with *Privacy by Design* – embed privacy into the design specifications of information technologies, accountable business practices and operations;
- Take it a step further – change the paradigm from “zero-sum” to “positive-sum,” where both privacy *and* security can be delivered, thereby raising the *overall* level of protection;
- When you change the paradigm, you then change the mindset: you can deliver *both* privacy AND security, not as mutually exclusive “either/or” (false dichotomy) but also doubly enabling “win/win;”
- The future of privacy may very well depend on embedding privacy into Design – let’s make it a reality!



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

For more information on *Privacy by Design*, please visit:

www.privacybydesign.ca