

***Find Ways to Deliver Both  
Security and Privacy***

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

*Canadian Society for Industrial Security*

*May 30, 2011*

# Presentation Outline

- 1. The IPC: Who We Are*
- 2. We Need to Change the Paradigm*
- 3. Information Privacy Defined*
- 4. Privacy  $\neq$  Security: You Need Both*
- 5. Privacy by Design: The Gold Standard*
- 6. PbD in Action: Video Surveillance*
- 7. Conclusions*



**The IPC:**  
*Who We Are*

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# IPC Mandate

**Under our statutory mandate, the IPC is responsible for:**

- Investigating privacy complaints;
- Resolving appeals from refusals to provide access to information;
- *Ensuring that organizations comply with the access and privacy provisions of the Acts;*
- *Educating the public and raising awareness of Ontario's access and privacy laws;*
- *Conducting research on access and privacy issues; providing advice and comment on proposed government legislation and programs.*

# Commissioner's Powers

**The Commissioner has the power to:**

- *Offer comment on the privacy protection implications of proposed programs of institutions;*
- In appropriate circumstances, authorize the collection of personal information otherwise than directly from the individual;
- *Engage in or commission research into matters affecting the carrying out of the purposes of the Acts;*
- *Conduct public education programs and provide information concerning this Act and the Commissioner's role;*
- Receive representations from the public concerning the operation of the Acts;
- Order the disclosure of government-held information.

# IPC: Three Statutes

The role of the Information and Privacy Commissioner of Ontario (IPC) is set out in three statutes:

- *Freedom of Information and Protection of Privacy Act (FIPPA);*
- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);*
- *Personal Health Information Protection Act (PHIPA).*



***Setting the Stage:  
Why We Need to  
Change the Paradigm***

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# Information Privacy Defined

## Information Privacy: Data Protection

- Freedom of choice; personal control; informational self-determination;
- Control over the collection, use and disclosure of any recorded information about an identifiable individual;
- Privacy principles embodied in “Fair Information Practices;”
- Global Privacy Standard (2006).  
[www.ipc.on.ca/images/Resources/up-gps.pdf](http://www.ipc.on.ca/images/Resources/up-gps.pdf)

# *What Privacy is Not*

**Privacy  $\neq$  Security**

*Security is, however, vital to privacy:  
You cannot have Privacy without Security*

[www.privacybydesign.ca](http://www.privacybydesign.ca)

**What is Needed is:**

**Privacy**

*and*

**Security,**

*not*

**one, to the exclusion of the other**

[www.privacybydesign.com](http://www.privacybydesign.com)

# The Future of Privacy

*Change the Paradigm to  
Positive-Sum,  
**NOT**  
Zero-Sum*

# 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 ...*

*replace the “vs.” with “and”*

# *The Decade of Privacy by Design*



[www.privacybydesign.ca](http://www.privacybydesign.ca)

# **Privacy by Design:** *The Trilogy of Applications*

**Information  
Technology**

**Accountable  
Business Practices**

**Physical Design  
& Networked  
Infrastructure**

# *Privacy by Design:* *The 7 Foundational Principles*

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



## Privacy by Design

### *The 7 Foundational Principles*

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

*Privacy by Design* is a concept 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* advances the view 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 realize that a more substantial approach is required — extending the use of PETs to *PETS Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in *PETS Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

*Privacy by Design* extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked 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 measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles (*see over page*):



***PbD in Action:  
Video Surveillance***

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# IPC Guidelines on Video Surveillance Cameras

My office has issued guidelines regarding the use of video surveillance cameras:

- *(Updated) Guidelines for the Use of Video Surveillance Cameras in Public Places (2007) - [www.ipc.on.ca/images/Resources/video-e.pdf](http://www.ipc.on.ca/images/Resources/video-e.pdf)*
- *Guidelines for the Use of Video Surveillance Cameras in Public Places (2001) - [www.ipc.on.ca/images/Resources/video-e.pdf](http://www.ipc.on.ca/images/Resources/video-e.pdf)*
- *Guidelines for Using Video Surveillance Cameras in Schools (2003) - [www.ipc.on.ca/images/Resources/vidsch-e.pdf](http://www.ipc.on.ca/images/Resources/vidsch-e.pdf)*

# IPC Guidelines for Video Surveillance Cameras in Public Places

- Collection of personal information;
- Prior considerations;
- Developing the policy;
- Designing and installing;
- Use, disclosure, retention, security and destruction;
- Audit and evaluation.

Information  
and Privacy  
Commissioner of  
Ontario

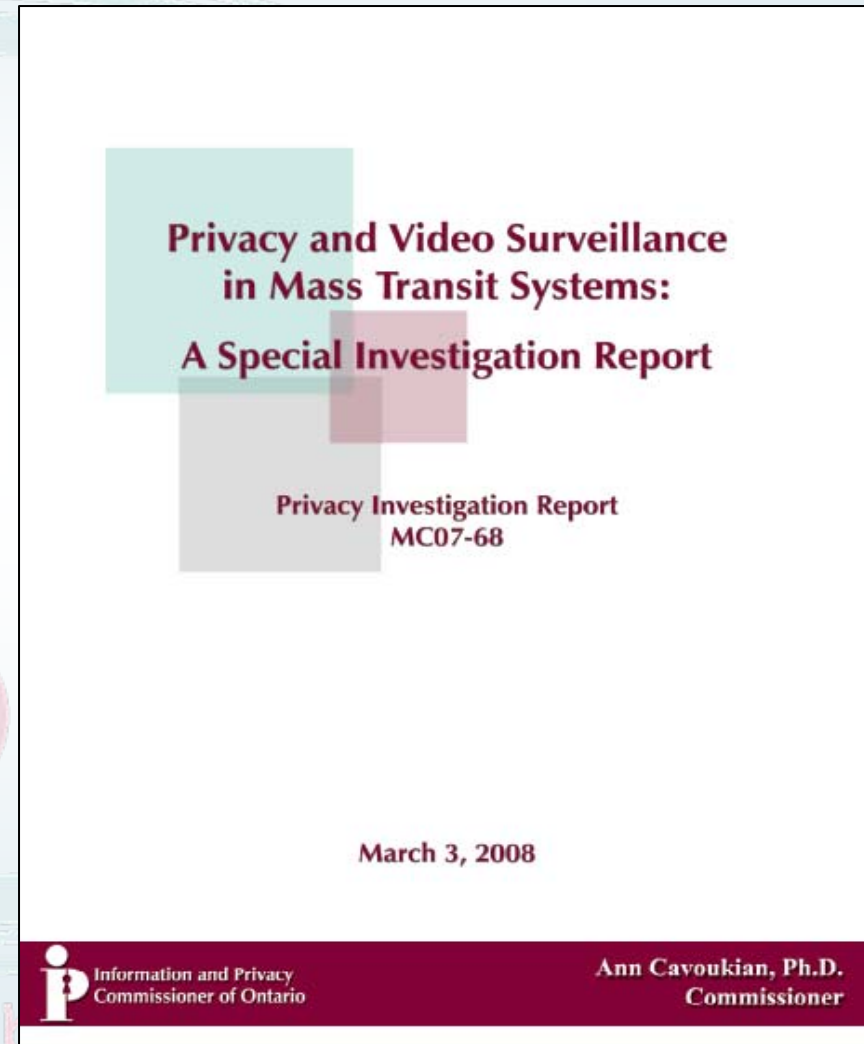
Guidelines for the Use of  
Video Surveillance Cameras  
in Public Places



Ann Cavoukian, Ph.D.  
Commissioner  
September 2007

# 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).



# TTC Surveillance Cameras

## *Privacy-Enhancing Technologies*

- An important part of the report is dedicated to the area of emerging privacy-enhancing video surveillance technology.

*“In light of the growth of surveillance technologies, not to mention the proliferation of biometrics and sensing devices, the future of privacy may well lie in ensuring that the necessary protections are built right into their design. Privacy by design may be our ultimate protection in the future, promising a positive sum paradigm instead of the unlikely obliteration of a given technology.”*

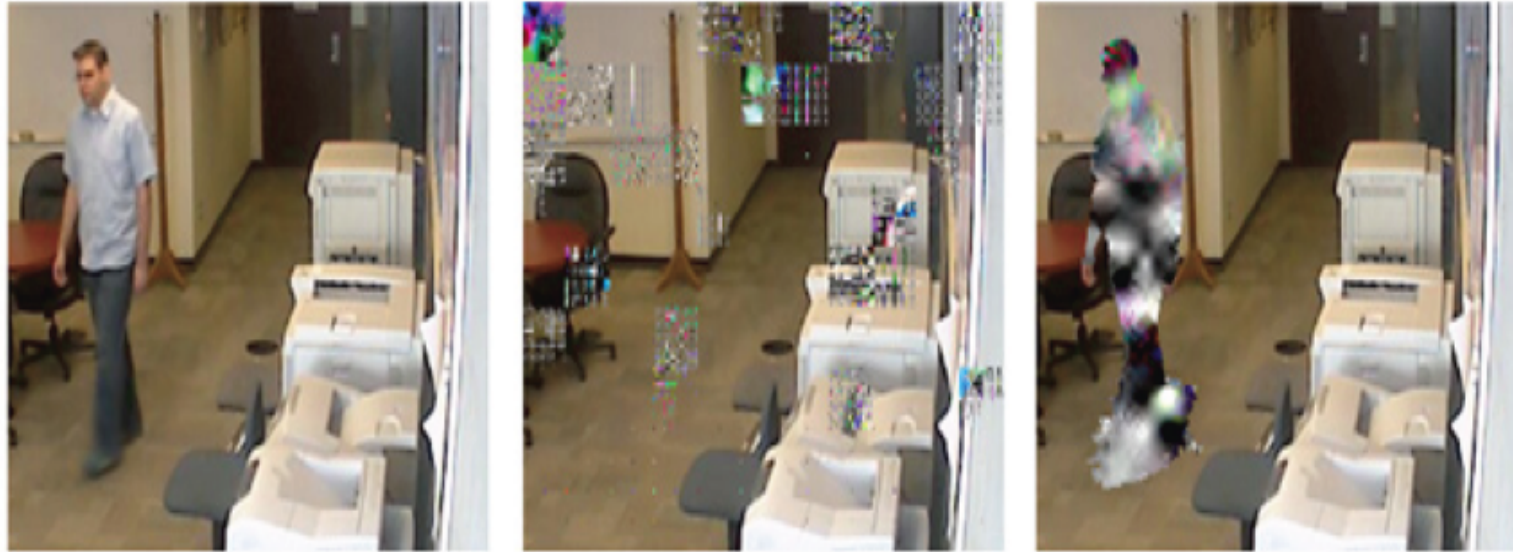
— *Privacy and Video Surveillance in Mass Transit Systems:  
A Special Investigation Report, March 2008*

# CCTV Cameras:

## *Innovative Privacy-Enhancing Approach to Video Surveillance*

- At the University of Toronto, Professor Kostas Plataniotis and Dr. 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.

# Conclusions

- Lead with *Privacy by Design*;
- Change the paradigm from the dated “zero-sum” to the doubly-enabling “positive-sum;”
- Deliver *both* privacy AND security in an empowering “win-win” paradigm;
- Get rid of the “vs.” – replace it with “and;”
- Embed privacy as a core functionality: deliver both privacy and security, not one at the expense of the other.

# 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](http://www.ipc.on.ca)**

**E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)**

**For more information on *Privacy by Design*,  
please visit: [www.privacybydesign.ca](http://www.privacybydesign.ca)**