

***Don't Sacrifice Privacy for Security:  
You Need Both – Privacy by Design***

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

*Government of Ontario Security Services  
and Contingency Planning Branch*

*May 31, 2011*

# Public Safety is Paramount: *But Balanced Against Privacy*

## Public safety is paramount – but balanced against privacy

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



*Since the attacks on the United States, there's been much talk of tightening up security – even at the expense of people's privacy. Pundits and politicians have suggested new compulsory identity cards, more widespread use of face-recognition software, loosening of the rules restricting wiretaps and other forms of eavesdropping, and tighter regulations at borders and on international flights.*

*What could be the impact on individual privacy? And what should be considered as we move forward? CBC News Online went to Ann Cavoukian for some perspective. She's the Information and Privacy Commissioner for Ontario, and author of *Who Knows: Safeguarding Your Privacy in a Networked World*.*

— September 21, 2001

None of us could have anticipated or imagined what happened on September 11. It was unthinkable. The attacks will undoubtedly have a significant impact on our lives, in ways we can't yet imagine. And one area that will be closely looked at is privacy: the extent to which certain of our fundamental freedoms and liberties may need to be compromised, in order to ensure these horrific acts aren't repeated.

Understandably, the law enforcement community is already calling for greater access to controversial new technologies, including Internet wiretaps, global communications-monitoring systems, face-recognition and fingerprint-scanning devices. In the United States, steps have already been taken in this direction. For example, the U.S. Senate passed an anti-terrorism bill that allows the government greater liberty to use surveillance technology to combat terrorism. And the attorney general, John Ashcroft, has sent a proposal to Congress to change wiretap rules to make it easier to track suspected terrorists. Inevitably, similar initiatives will be considered in Canada.

At the heart of this debate is the balance between human rights and civil liberties, including privacy, and the intrusion on these rights in the name of public safety. We may have to rethink this balance. And that should come as no surprise. The balance between security and privacy has never been static, shifting in favour of security whenever we're faced with significant threats to public safety.

But let us return to first principles.

Privacy is not an absolute right (no right is absolute). There have always been situations where personal privacy has given way to legitimate law enforcement and public safety concerns. These unprecedented terrorist attacks may have changed our perceptions and firmly-held notions of what constitutes realistic threats to public safety. Consequently, as a society, we may be willing to accept greater intrusions into our personal lives in order to ensure our collective security.

*CBC Online*

*September 21, 2001*

# Presentation Outline

- 1. Privacy is Essential to Freedom*
- 2. We Need to Change the Paradigm*
- 3. Privacy  $\neq$  Security*
- 4. Positive-Sum, NOT Zero-Sum*
- 5. Privacy by Design: The Gold Standard*
- 6. PbD in Action: Video Surveillance Cameras*
- 7. Conclusions*



***Privacy = Freedom***

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

***Setting the Stage:***

***Why We Need to  
Change the Paradigm***

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

# *What Privacy is Not*

**Privacy  $\neq$  Security**

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

**What is Needed is:**

**Privacy**

*and*

**Security,**

*not*

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

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

# The Future of Privacy

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

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

# **A Matter of Balance?**

## ***The Trouble with “Balance” Metaphors***

**Julian Sanchez**

**[www.juliansanchez.com](http://www.juliansanchez.com)**

***Inspired by Orin Kerr’s paper on an  
equilibrium-adjustment theory of the Fourth Amendment***

# *The Trouble with “Balance” Metaphors*

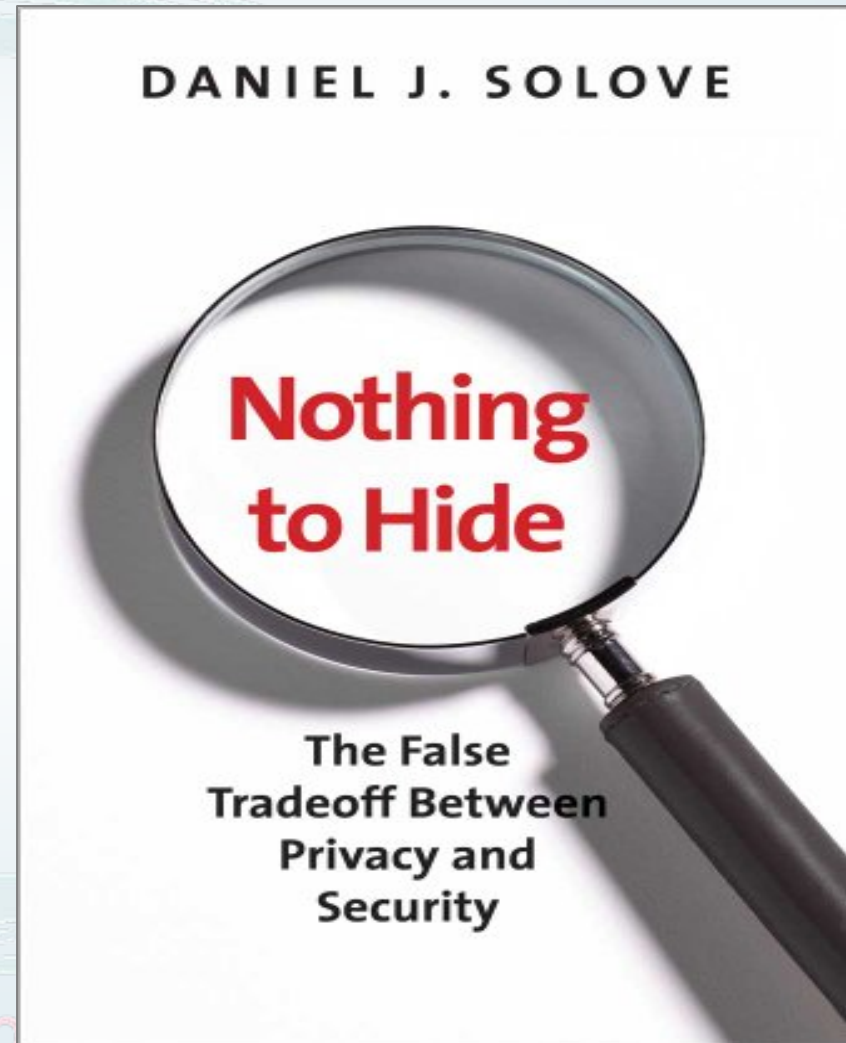
*“ ... the most obvious problem with balancing metaphors is that they suggest a relationship that is always, by necessity, zero sum: If one side rises, the other must fall, in exact proportion.”*

— Julian Sanchez, February 14, 2011.

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

# *Nothing to Hide: The False Tradeoff between Privacy and Security*

*“The debate between privacy and security has been framed incorrectly as a zero-sum game in which we are forced to choose between one value and the other. Why can't we have both?”*



# Positive-Sum Model

*Change the paradigm  
from a zero-sum to  
a “positive-sum” model:  
Create a win-win scenario,  
not an either/or (vs.)  
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*):

# *Adoption of “Privacy by Design” Resolution*

## **Landmark Resolution Passed to Preserve the Future of Privacy**

By Anna Ohlden – October 29th 2010 - [http://www.science20.com/newswire/landmark\\_resolution\\_passed\\_preserve\\_future\\_privacy](http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy)

**JERUSALEM, October 29, 2010** – A landmark Resolution by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, was approved by international Data Protection and Privacy Commissioners in Jerusalem today at their annual conference. The resolution recognizes Commissioner Cavoukian's concept of Privacy by Design - which ensures that privacy is embedded into new technologies and business practices, right from the outset - as an essential component of fundamental privacy protection.

### **Full Article:**

[http://www.science20.com/newswire/landmark\\_resolution\\_passed\\_preserve\\_future\\_privacy](http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy)



## Privacy by Design Resolution

### 32nd International Conference of Data Protection and Privacy Commissioners

27-29 October 2010, Jerusalem, Israel

#### Proposer:

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

#### Co-sponsors:

Jennifer Stoddart  
Privacy Commissioner of Canada

Dr. Alexander Dix  
Commissioner for Data Protection & Freedom of Information, Berlin, Germany

Igor Némec  
President, Office for Personal Data Protection, Czech Republic

Dr. Viljar Peep  
Director General, Estonian Data Protection Inspectorate

Marie Shroff  
Privacy Commissioner, New Zealand

Knowing that with technological advances come new challenges to privacy and to the ability of individuals to exercise their information rights effectively;

Accepting that existing regulation and policy alone are not sufficient fully to safeguard privacy;

Understanding that a more robust approach is required to address the ever-growing and systemic effects of Information and Communication Technologies (ICT), and of large-scale networked infrastructure;

Recognizing that embedding privacy as the default into the design, operation and management of ICT and systems, across the entire information life cycle, is necessary to fully protect privacy;

Offering *Privacy by Design* as a holistic concept that may be applied to operations throughout an organization, end-to-end, including its information technology, business practices, processes, physical design and networked infrastructure;

The 32nd International Conference of Data Protection and Privacy Commissioners gathered at Jerusalem therefore resolves to:

1. Recognize *Privacy by Design* as an essential component of fundamental privacy protection;
2. Encourage the adoption of the Foundational Principles of *Privacy by Design*, such as those set out below as guidance to establishing privacy as an organization's default mode of operation;
3. Invite Data Protection and Privacy Commissioners/Authorities to:
  - a. promote *Privacy by Design*, as widely as possible through distribution of materials, education and personal advocacy;
  - b. foster the incorporation of the *Privacy by Design* Foundational Principles in the formulation of privacy policy and legislation within their respective jurisdictions;
  - c. proactively encourage research on *Privacy by Design*;
  - d. consider adding *Privacy by Design* to the agendas of events taking place on International Data Privacy Day (January 28);
  - e. report back to the 33<sup>rd</sup> International Data Protection and Privacy Commissioners Conference, where appropriate, on *Privacy by Design* activities and initiatives undertaken within their jurisdictions with a view to sharing best practices.

#### *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 Security — Lifecycle Protection*
6. *Visibility and Transparency*
7. *Respect for User Privacy*

#### *Explanatory Note*

The right to control the collection, use and disclosure of information about oneself is an essential foundation upon which free societies are built. Technological advances have brought new challenges to this right and individuals' ability to exercise it effectively. Regulation and policy are no longer sufficient to safeguard privacy. With the increasing complexity and interconnectedness of information technologies, nothing short of building privacy directly into system design and processes can suffice.

The concept of "*Privacy by Design*" was developed to address the ever-growing and systemic effects of Information and Communication Technologies (ICT), and of large-scale networked infrastructure, in a comprehensive manner. *Privacy by Design* refers to the philosophy and approach of embedding privacy into the design, operation and management of information technologies and systems, across the entire information life cycle.

The Foundational Principles of *Privacy by Design* set out how to proactively make privacy the default mode of operation across an organization, while maintaining full functionality — a positive-sum, not zero-sum, approach to privacy protection.

# *Privacy by Design in 2010: Gathering Momentum*

- **May** – As part of the European Commission’s new European Digital Agenda, **Peter Hustinx**, the European Data Protection Supervisor, recommended that *Privacy by Design* be included as a binding principle into data protection legal framework;  
[www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19\\_Trust\\_Information\\_Society\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf)
- **October** – Regulators from around the world gathered at the annual assembly of **International Data Protection and Privacy Commissioners** in Jerusalem, Israel, and unanimously passed a landmark Resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection;  
[www.privacylaws.com/templates/EnewsPage.aspx?id=1663](http://www.privacylaws.com/templates/EnewsPage.aspx?id=1663)
- **December** – The **U.S. Federal Trade Commission** released a major report on protecting consumer privacy in which it recommended that companies adopt a *Privacy by Design* approach by building privacy protections into their everyday business practices.  
[www.privacybydesign.ca/media-centre/in-the-news/](http://www.privacybydesign.ca/media-centre/in-the-news/)

# *Privacy by Design in 2011 ...*

## *We're Just Getting Started*

- **February** – Debate in Dutch Senate began with a panel of experts deliberating data protection and privacy – consistently referring to the need for *Privacy by Design*, the first *PbD* certified consulting method for biometric identity systems being contemplated;
- **February** – Japan's Ministry of Economy, Trade and Industry translated the *Privacy by Design Foundational Principles* (on the heels of a Chinese translation), and is now replicating our *PbD* Ambassador Program in Japan;
- **April** – U.S. Senators John Kerry and John McCain cited *Privacy by Design* in their *Commercial Privacy Bill of Rights* that requires businesses that collect, use, store or transfer consumer information to implement data privacy protections when developing products and provide consumers with choices about how data are used, collected and shared.

# *Privacy by Design:* **Proactive in 21 Languages!**

- |                  |                    |                      |
|------------------|--------------------|----------------------|
| <i>1.English</i> | <i>8.Estonian</i>  | <i>15.Korean</i>     |
| <i>2.French</i>  | <i>9.Hebrew</i>    | <i>16.Ukrainian</i>  |
| <i>3.German</i>  | <i>10.Hindi</i>    | <i>17.Russian</i>    |
| <i>4.Italian</i> | <i>11.Chinese</i>  | <i>18.Romanian</i>   |
| <i>5.Spanish</i> | <i>12.Japanese</i> | <i>19.Portuguese</i> |
| <i>6.Czech</i>   | <i>13.Arabic</i>   | <i>20.Maltese</i>    |
| <i>7.Dutch</i>   | <i>14.Armenian</i> | <i>21.Greek</i>      |



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

[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)*
- **December 2007** – the IPC was invited by the U.S. Department of Homeland Security to speak on best practices for CCTV programs.

# IPC Guidelines for Video Surveillance Cameras in Public Places

- Applies only to 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

# Toronto Police Services

## *Surveillance Cameras*

- The Toronto Police Service (TPS) conducted a pilot project testing Closed Circuit Television (CCTV) in specific high-crime areas, as an added tool for the detection and deterrence of crime and enhancing public safety and security;
- In August 2006, members of the TPS met with the Commissioner and IPC staff 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 TPS kept the IPC informed of developments during the program, which concluded in Spring 2008.

# Toronto Police Services

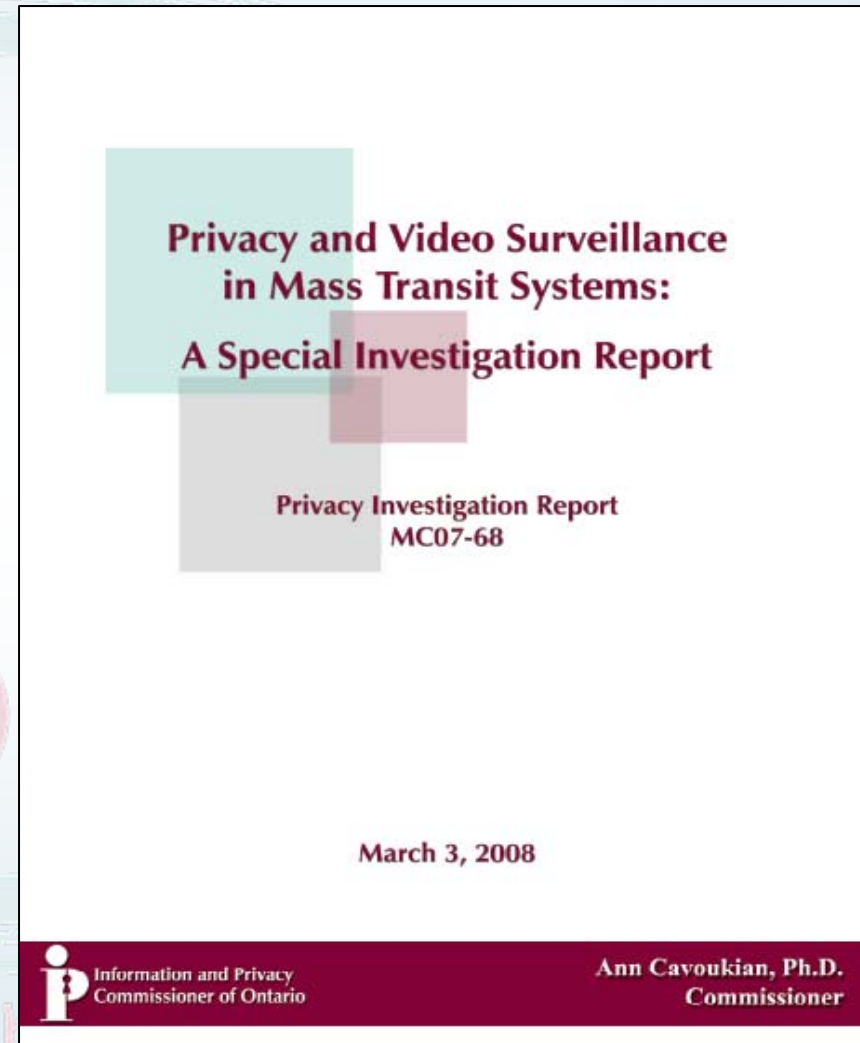
## *Support for Positive-Sum*

“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.

# 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 must be conducted by an independent third party using the Generally Accepted Privacy Principles;
  - Two-signature sign-off is key!



# 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.”*

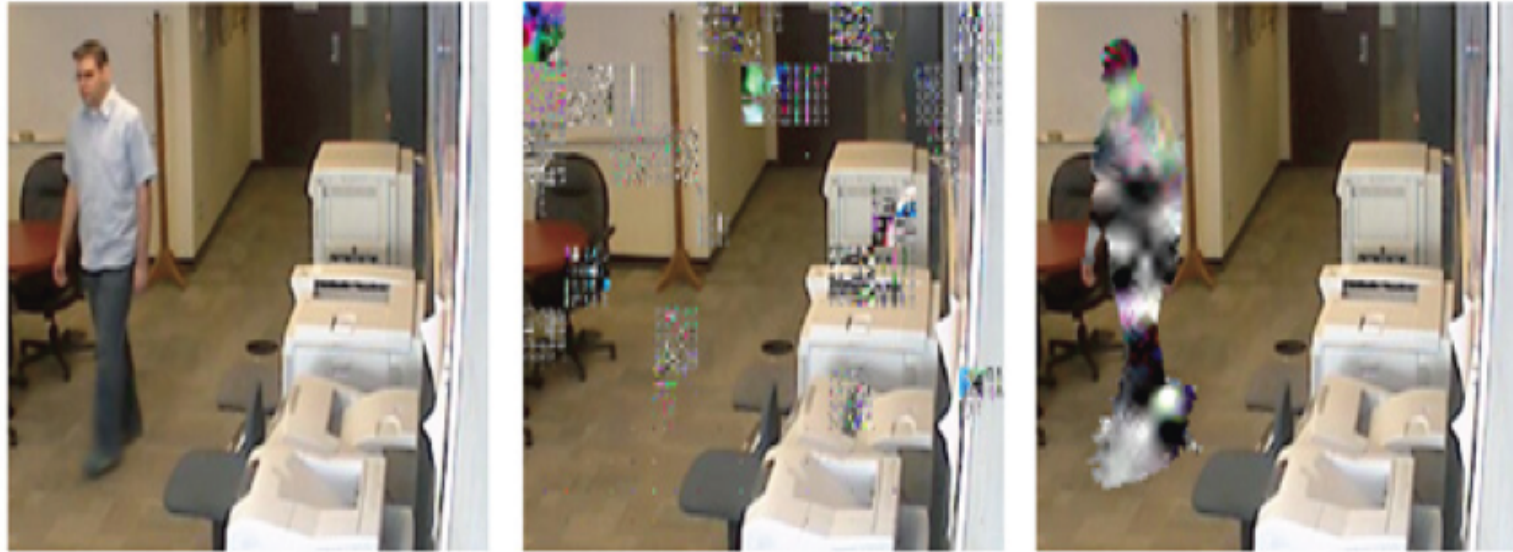
— *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report, March 2008*

# 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.

# IPC Philosophy

## *The 3 C's*

**My office tries to actively engage in the 3 C's:**

- **Consultation:**  
by keeping open the lines of communication;
- **Co-operation:**  
rather than confrontation, in resolving complaints;
- **Collaboration:**  
by working together and seeking partnerships  
to find joint solutions.

# Conclusions

- Lead with *Privacy and Security, 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)**