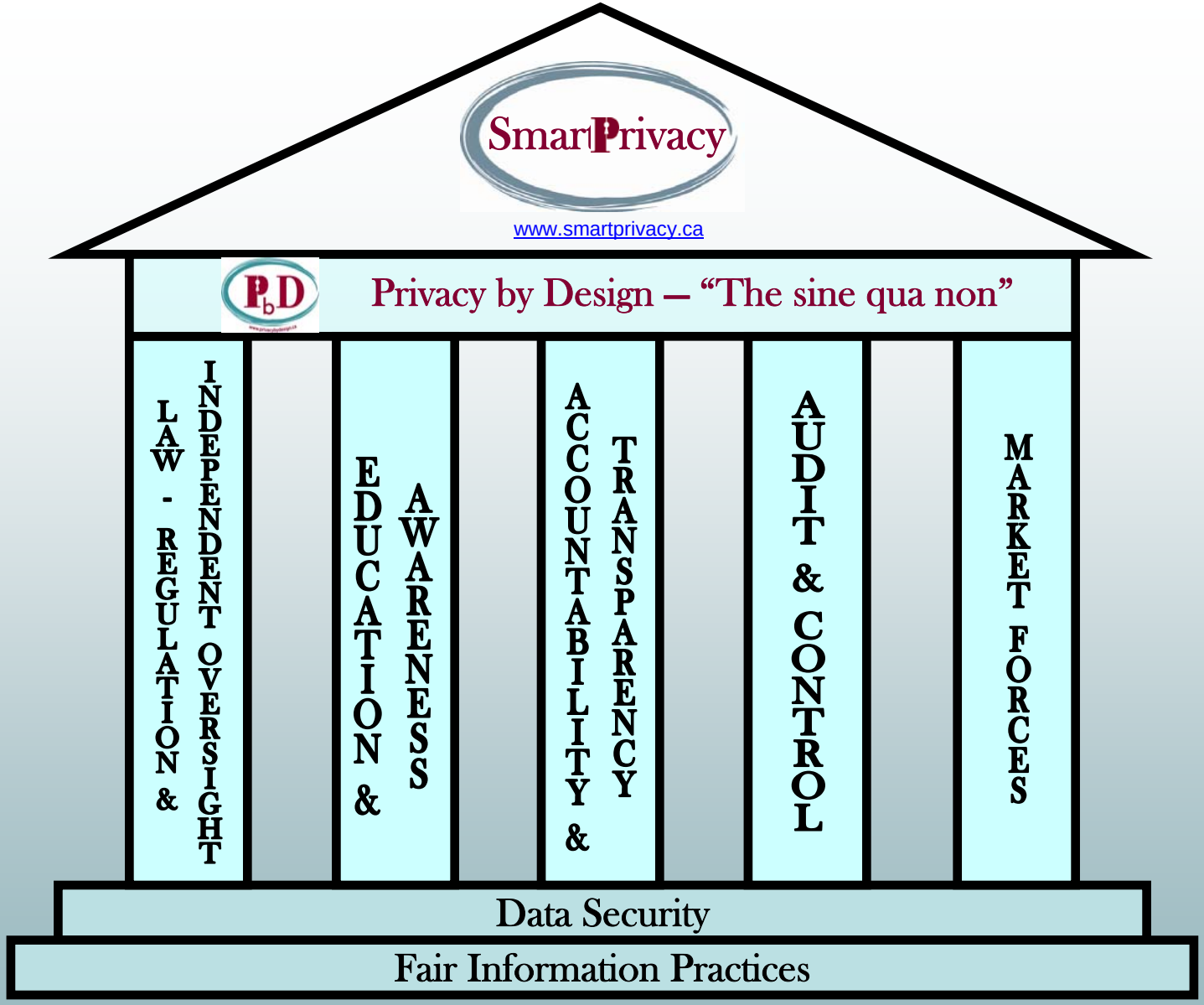
SmartPrivacy for Smart Public Safety

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Toronto Forum for Global Cities Conference
Smarter Public Safety Panel
November 10, 2009

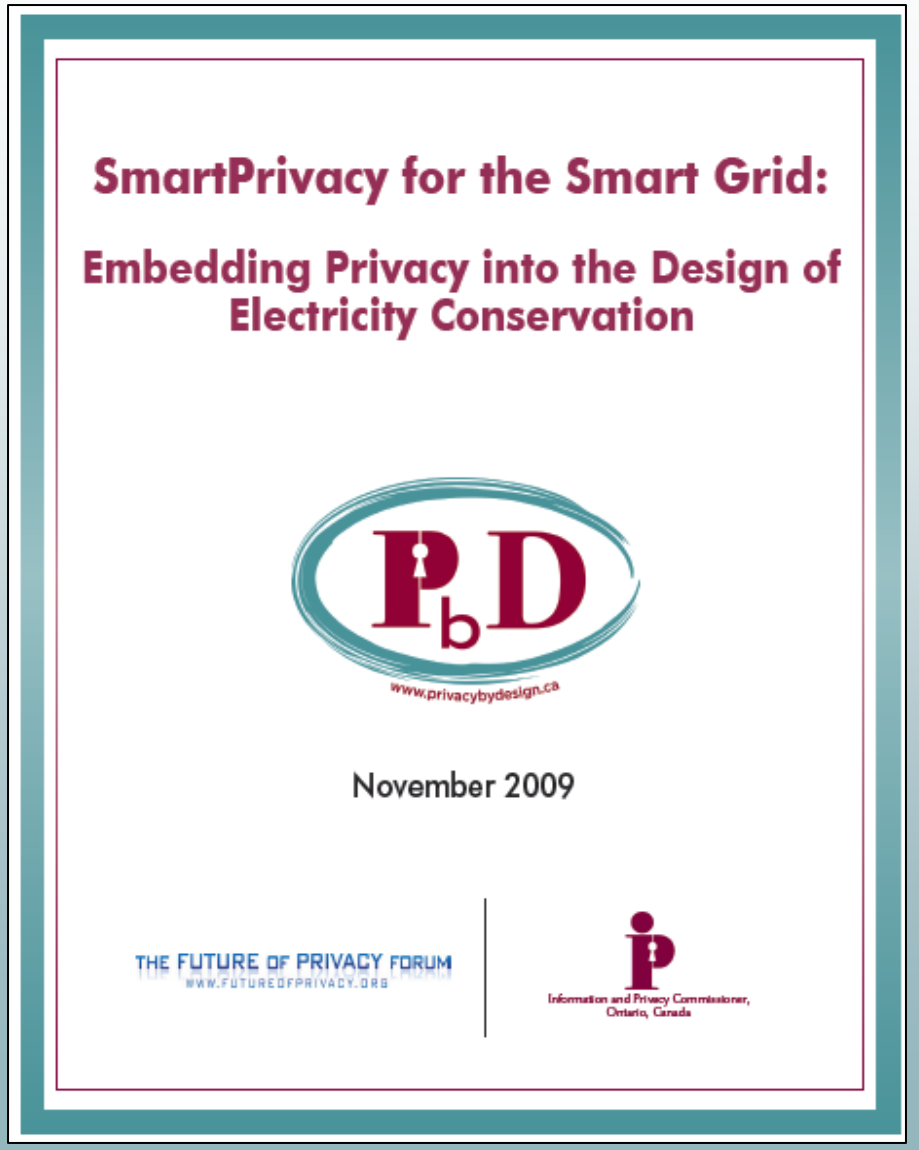


"SmartPrivacy is the umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protections to education and awareness, but one measure stands out as the sine qua non: *Privacy by Design*. *Dr. Ann Cavoukian, Information & Privacy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

SmartPrivacy for the Smart Grid

- To be released on November 17, 2009, with the Future of Privacy Forum.

  www.privacybydesign.ca

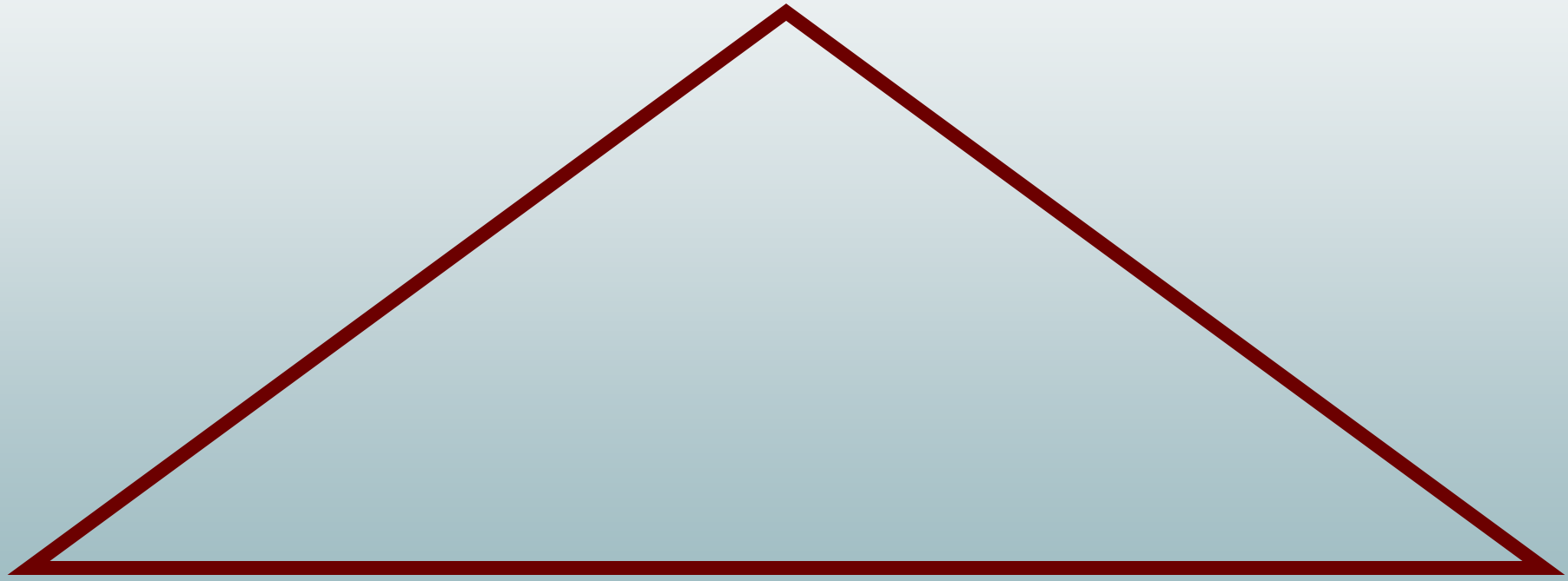



PbD
www.privacybydesign.ca

Privacy by Design: "Build It In"

- I first developed the term "Privacy by Design" back 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



Positive-Sum

not

Zero-Sum

Positive-Sum Paradigm

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

Positive-Sum Model

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

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.

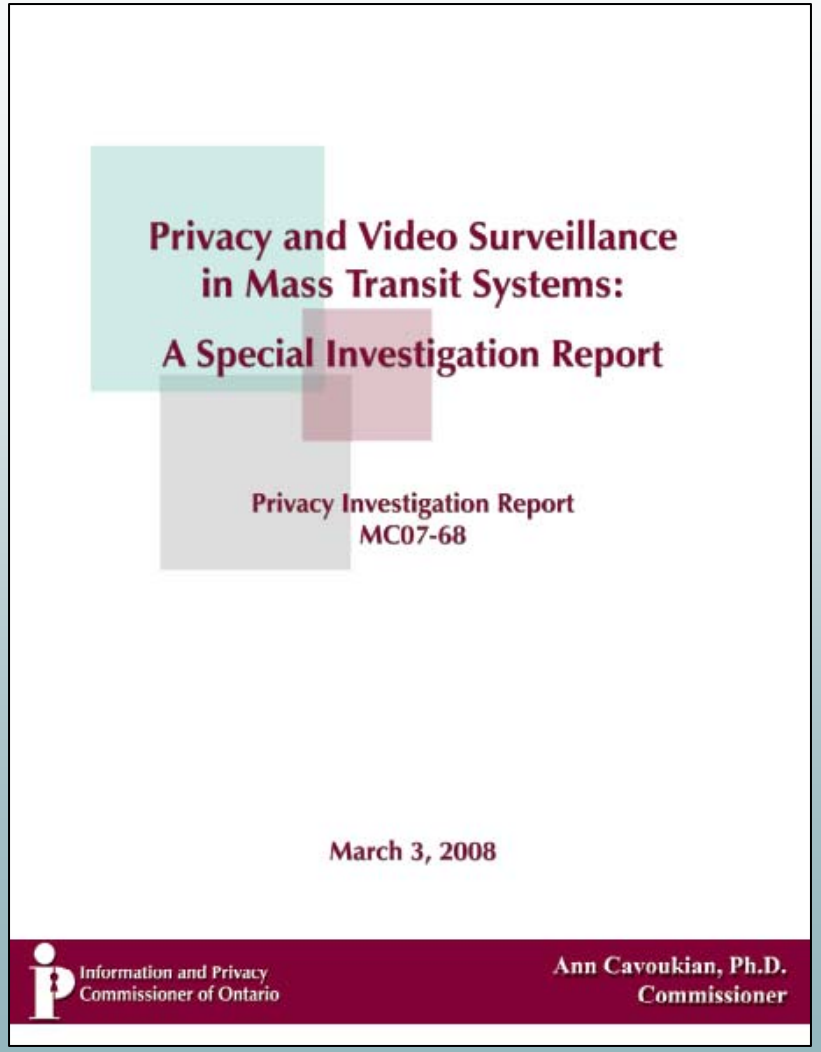
Privacy by Design:
The 7 Foundational Principles

No. 4: Full Functionality – Positive-Sum, not Zero-Sum

- *Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy ***vs.*** security, demonstrating that it ***is*** possible to have both.

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).

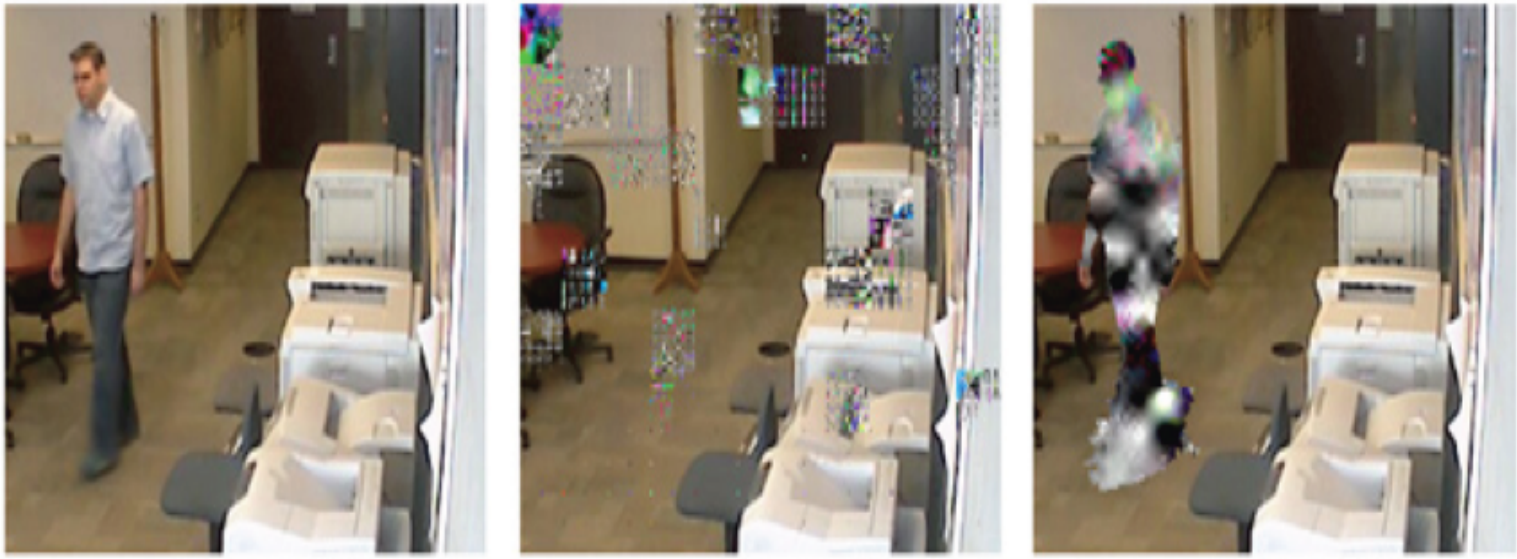


www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf

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

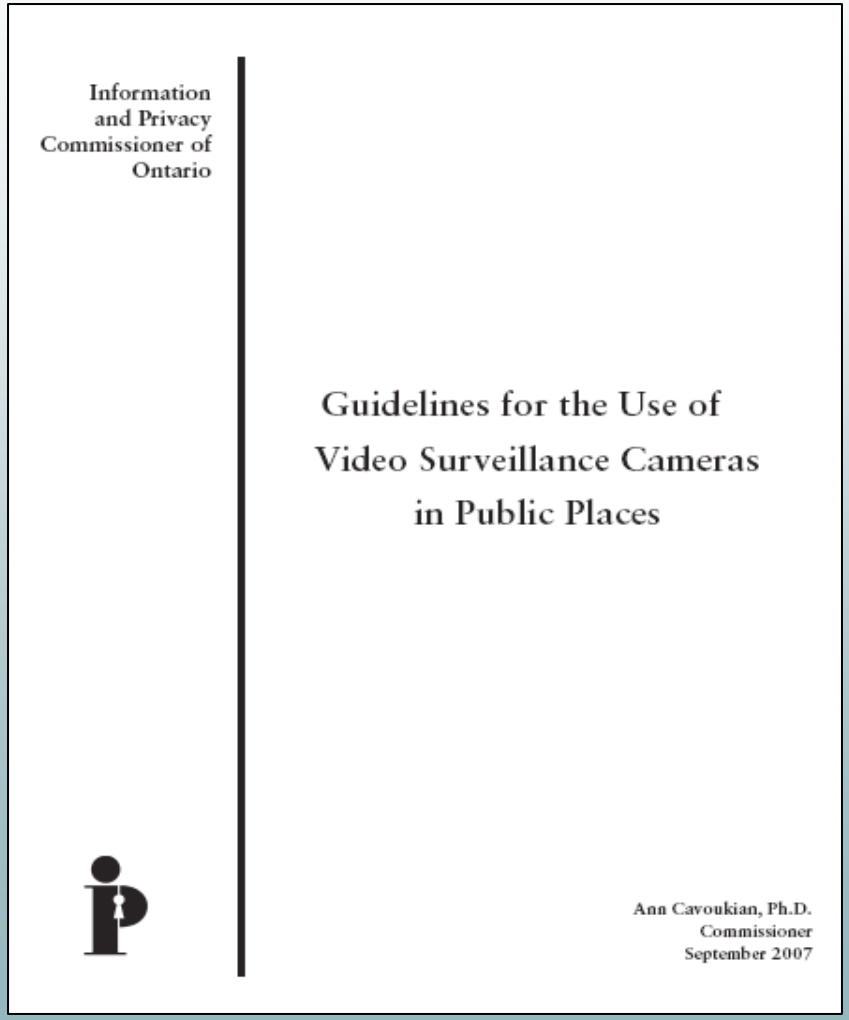


(a) (b) (c)

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.

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.



www.ipc.on.ca/images/Resources/video-e.pdf

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.

Conclusions

- Lead with ***Privacy by Design*** – embed privacy into the design specifications of various technologies, business practices and operations;
- Change the paradigm from "zero-sum" to "positive-sum," where both privacy *and* security or any functionality can be delivered, thereby raising the *overall* level of protection;
- When you change the paradigm, you change the mindset: you can deliver *both* privacy AND security/public safety, not the mutually exclusive "either/or" (false dichotomy);
- The future of privacy may very well depend on embedding privacy into design – let's make it a reality – let's get **Smart** about privacy.

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