Technology-Related Orders and Investigations

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

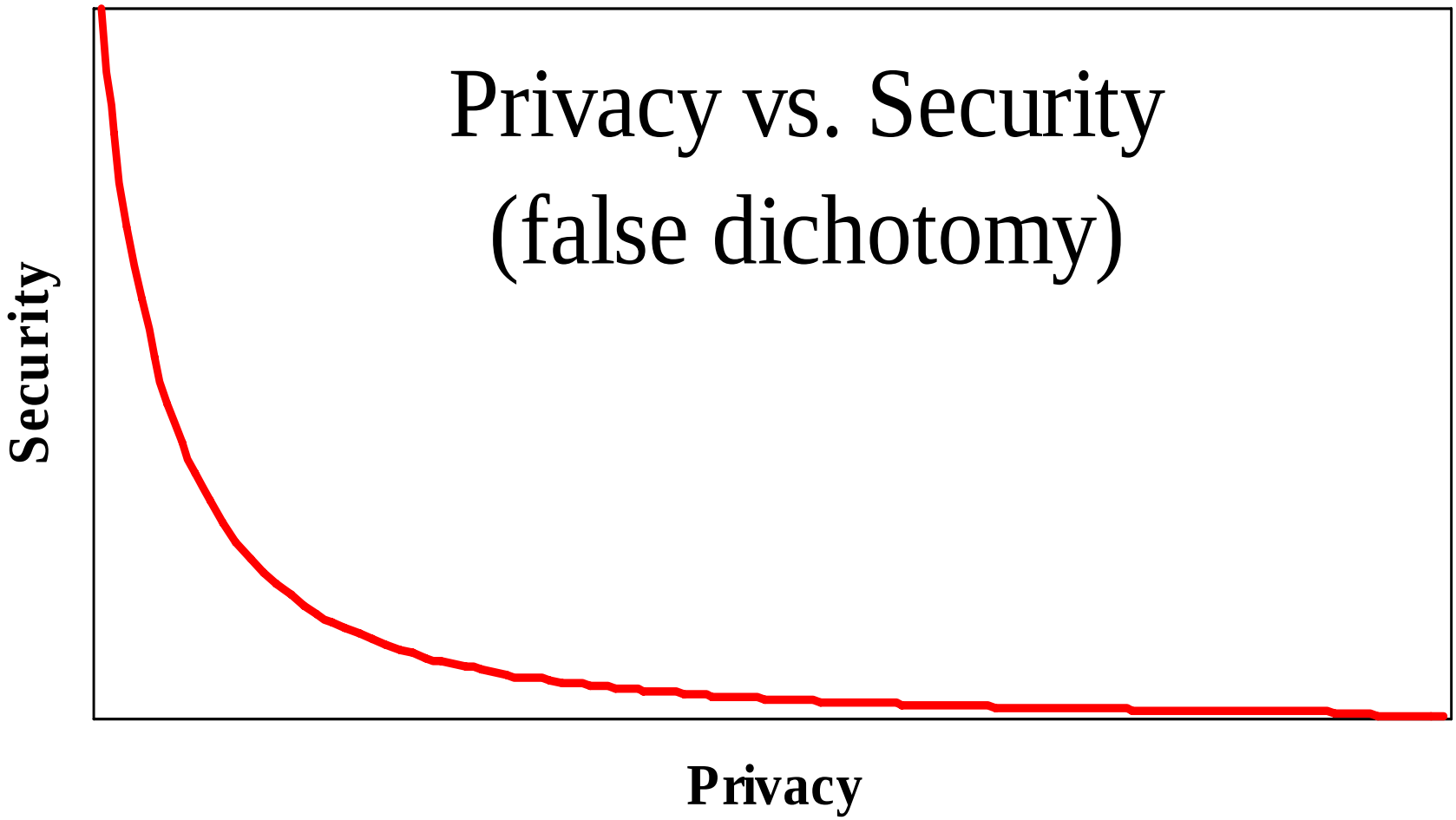
AICPA/CICA Task Force
Toronto, Canada
May 7, 2008

Presentation Outline

1. *Positive-Sum NOT Zero-Sum*
2. *Transformative Technologies*
3. *Video Surveillance Cameras*
4. *IPC Technology-Related Orders*
5. *Biometric Encryption*
6. *Radio Frequency Identification*
7. *Enhanced Driver's Licenses*

Positive-Sum
NOT
Zero-Sum

Privacy OR Security:
A Zero-Sum Game



Positive-Sum Model

Change the paradigm
from a zero-sum to
a positive-sum model:
Create a "win-win" scenario

Looking at Privacy Differently

Old World: Zero-sum mentality

Future: Positive-sum paradigm

Don't get stuck in the past

Transformative Technologies

Privacy-Invasive Technologies

- There are an ever growing number of technologies that give rise to ongoing concerns regarding privacy and the protection of personal information – especially given their ***privacy invasive*** nature and tendency towards facilitating surveillance.
  - Biometrics
  - Radio Frequency Identification (RFID)
  - Video Surveillance Cameras
  - Identity Management

The Power of Transformative Technologies

- However, by applying a positive-sum paradigm, any technology can be built with privacy in mind transforming them from a privacy-invasive technology to a privacy-protective technology.
- This can be seen in many joint-projects that the IPC has worked on such as:
  - RFID in Health Care (Hewlett-Packard)
  - Biometric Encryption (Philips)
  - Mass Transit Surveillance Cameras
  - Identity Management on the Internet
- This builds on our earlier work involving Privacy-Enhancing Technologies (PETs).

Privacy-Enhancing Technologies *(PETs)*

- The IPC developed 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 the landmark study, ***Privacy-Enhancing Technologies: The Path to Anonymity (Vols. I & II).***

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

Privacy by Design: "Build It In"

- Build in privacy – up front, into the design specifications into the architecture; if possible embed privacy right into the technology used – ***bake it in***;
- Assess the risks to privacy: conduct a privacy impact assessment; follow up with annual privacy audits;
- 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): give your customers maximum control over their data.

Privacy-Enhancing Technologies *(PETs)*

- Privacy-Enhancing Technologies include those that empower individuals to manage their own identities in a privacy enhancing manner.

- These include tools or systems to:
  - anonymize and pseudonymize identities;
  - securely manage login IDs and passwords and other authentication requirements;
  - restrict traceability and limit surveillance;
  - allow users to selectively disclose their Personally Identifiable Information (PII) to others and exert maximum control over their PII once disclosed.

Video Surveillance Cameras

Our Work On Video Surveillance

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

- *(Updated) Guidelines for the Use of Video Surveillance Cameras in Public Places* (2007) - 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
- *Guidelines for Using Video Surveillance Cameras in Schools* (2003) - 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 at a workshop on best practices for CCTV programs.

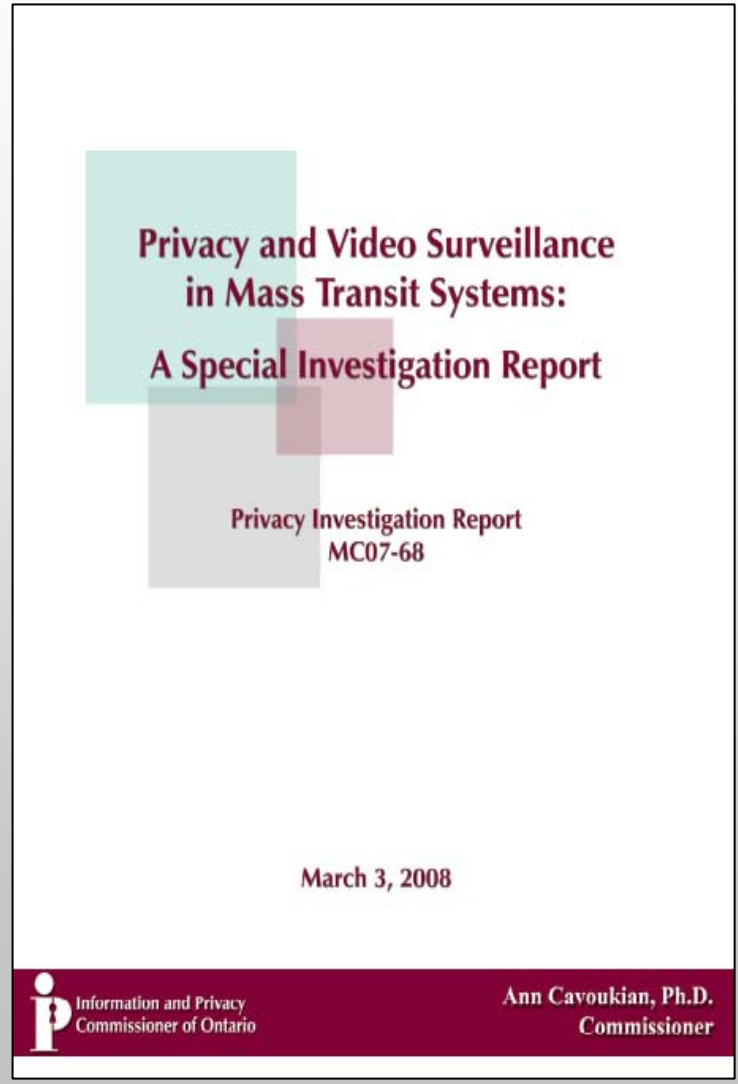
TTC Surveillance Cameras

- **October 2007** – Privacy International (U.K.) files a complaint with the IPC regarding the TTC's plan to implement 12,000 cameras across Toronto's transportation network of buses, streetcars, and subways citing that the TTC's plan contravened the privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA);
- **March 2008** – I ruled that the Toronto Transit System's expansion of its video Surveillance system, for the purposes of public safety, was in compliance with *MFIPPA*, but subject to strict controls.

TTC Surveillance Cameras

However, I recommended that the TTC undertake a number of specific measures to enhance privacy:

- Personal information will only be collected for legitimate, limited and specific purposes and retained for 15 to 72 hours only;
- Collection will be limited to the minimum necessary for the specified purposes; and
- Personal information will only be used and disclosed for the specified purposes.



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

TTC Surveillance Cameras
Further Recommendations

Overall, I made 13 recommendations to the TTC. Among those are:

- The retention period for video surveillance images be reduced from a maximum of seven days to a maximum of 72 hours;
- An annual third-party audit that is independent, thorough, comprehensive, and capable of testing all program areas of the TTC deploying video surveillance, using the Generally Accepted Privacy Principles (GAPP);
- A location to be selected to evaluate the privacy-enhancing video surveillance technology, identified in the report;
- Prior to providing the police with direct remote access to the video surveillance images, the TTC should amend the draft memorandum of understanding with the Toronto Police requiring that the logs of disclosures be subjected to regular audits.

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 sensoring 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

Surveillance Cameras
Work with University of Toronto

- University of Toronto researchers, Karl Martin and Kostas Plataniotis, have developed a privacy-enhancing approach to video surveillance;
- Their work, as described in *Privacy Protected Surveillance Using Secure Visual Object Coding*, uses cryptographic techniques to secure a private object so that it may only be viewed by designated persons of authority, by unlocking the encrypted object with a secret key;
- By using a secure object-based algorithm, you can not only securely obscure the faces of subway riders, for example, but if the faces are required for identification purposes, then they can be decrypted to reveal the faces;
- This allows designated persons to monitor the footage for unauthorized activity while strongly protecting the privacy of any individuals caught on tape. After an incident occurs that requires further investigation, the authorities can then decrypt the faces in order to identify the subjects in question.

TTC Surveillance Cameras Will Not Lead to a Police State

- Mass transit cameras are not only used for crime prevention, but also for crime detection and investigation;
- Police only have access to the footage ***after*** a crime has occurred;
- When police *do* request access to a tape, it is fully logged and audited;
- Tapes are automatically erased and overwritten, by default, within 15 to 72 hours;
- Video surveillance images are not actively monitored;
- Privacy-enhancing technologies can provide security and protect privacy.

What the Experts are Saying

“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, Director of the Indiana University Center for Applied Cybersecurity Research

“It sets the bench mark for informed discussion of CCTV in mass transit systems such as Toronto's. 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 of how they are introduced - this is the Commissioner flexing her muscles. Finally, it demonstrates that Canadian privacy laws have the capacity to meet technological challenges such as CCTV and 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 of PrivacyScan

IPC Technology-Related Orders

Personal Health Information Protection Act (PHIPA)

- Applies to organizations and individuals involved in the delivery of health care services (both public and private sector);
- The only health sector privacy legislation in Canada based on consent: implied consent within healthcare providers' "circle of care," otherwise, express consent;
- The only health sector privacy legislation that was declared to be substantially similar to Canada's federal private sector law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Health Order No. 2:
Unauthorized Access Results in Order

- **Health Order No. 2** (HO-02) showed that the hospital's policies and procedures failed to prevent ongoing privacy breaches by an employee, even after the hospital became aware that such breaches had occurred repeatedly;
- Even when the patient alerted the hospital to her concerns upon admission, the staff did not recognize the obvious threat to privacy posed by the estranged husband and his girlfriend- both employees of the hospital;
- Staff only recognized the threat to the physical security of the patient, not the threat to her privacy;
- After learning about the breach, the hospital was more concerned about the employee's right to due process (Human Resources Policy) than the patient's right to privacy;
- Hospitals can have both – but HR cannot trump privacy.

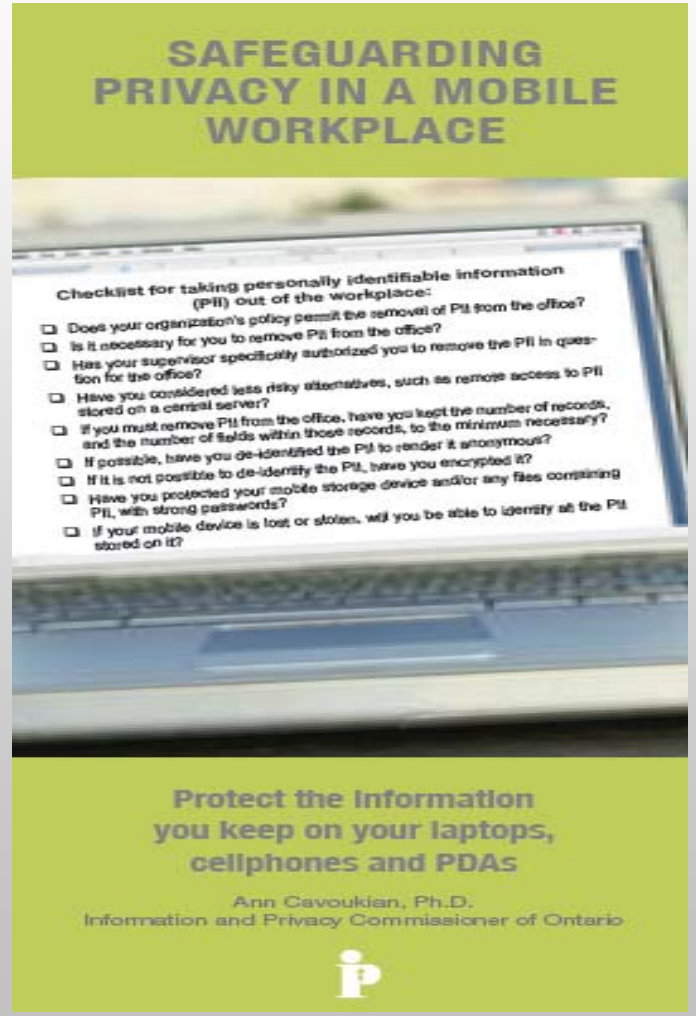
Health Order No. 4
Stolen Laptop Results in Order

- **Health Order No. 4** (HO-04) resulted from a hospital not having adequate policies and procedures to permit compliance with *PHIPA*;
- In spite of the known high risk of loss or theft, extremely sensitive personal health information was transported on a portable device (laptop) without adequate safeguards;
- This is clearly unacceptable, more than two years after *PHIPA* came into force.

Brochure on Mobile Devices

Safeguarding Privacy In A Mobile Workplace

- Does your organization's policy permit the removal of PII from the office?
- Is it necessary for you to remove PII from the office?
- Has your supervisor specifically authorized you to remove the PII in question for the office?
- Have you considered less risky alternatives, such as remote access to PII stored on a central server?
- If possible, have you de-identified the PII to render it anonymous?
- If it is not possible to de-identify the PII, have you encrypted it?
- If your mobile device is lost or stolen, will you be able to identify the PII stored on it?



www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf

Health Order No. 5

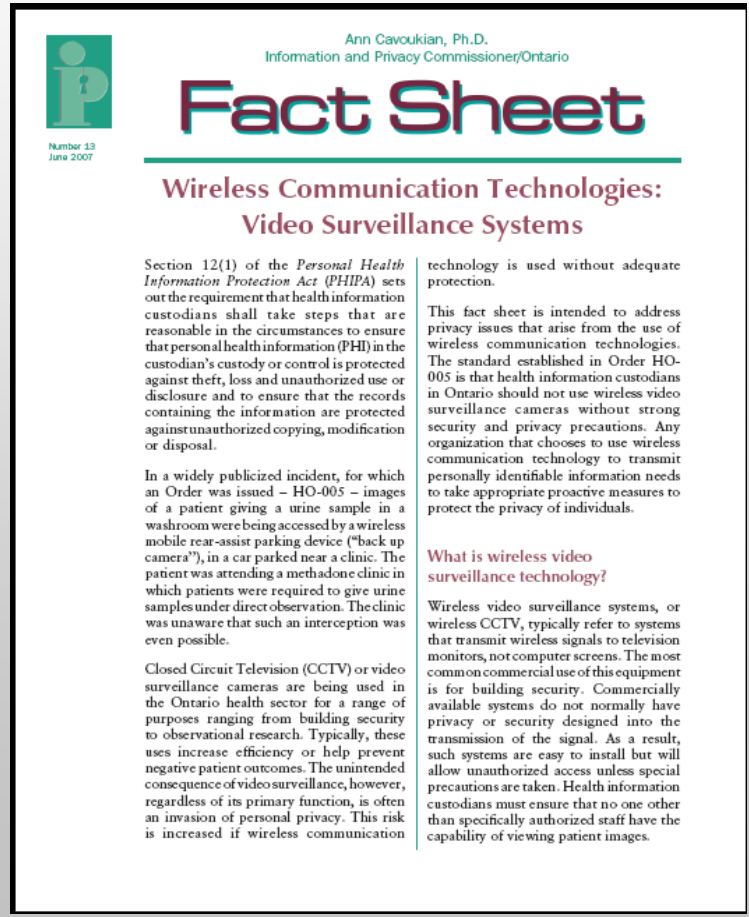
Wireless Technology Results in Order

- **Health Order No. 5** (HO-05) resulted from a methadone clinic that installed a wireless video surveillance system in its washroom to monitor patients providing urine samples;
- Video images were intercepted by a wireless rear view backup camera in a car outside of the clinic;
- Clinic immediately agreed to shut down the cameras and replaced the wireless surveillance system with a more secure wired system.

Fact Sheet

Wireless Communication Technologies: Video Surveillance Systems

- Special precautions must be taken to protect the privacy of video images;
- No covert surveillance should be conducted;
- Clearly visible signs should be posted indicating the presence of cameras and the location of their use;
- Recording devices should not be used;
- Only minimum number of staff should have access to the video equipment;
- Staff should receive technical training on the privacy and security issues;
- Regular security and privacy audits should be conducted, on an annual basis.



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

Fact Sheet

Number 13
June 2007

Wireless Communication Technologies: Video Surveillance Systems

Section 12(1) of the *Personal Health Information Protection Act* (*PHIPA*) sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

In a widely publicized incident, for which an Order was issued – HO-005 – images of a patient giving a urine sample in a washroom were being accessed by a wireless mobile rear-assist parking device ("back up camera"), in a car parked near a clinic. The patient was attending a methadone clinic in which patients were required to give urine samples under direct observation. The clinic was unaware that such an interception was even possible.

Closed Circuit Television (CCTV) or video surveillance cameras are being used in the Ontario health sector for a range of purposes ranging from building security to observational research. Typically, these uses increase efficiency or help prevent negative patient outcomes. The unintended consequence of video surveillance, however, regardless of its primary function, is often an invasion of personal privacy. This risk is increased if wireless communication technology is used without adequate protection.

This fact sheet is intended to address privacy issues that arise from the use of wireless communication technologies. The standard established in Order HO-005 is that health information custodians in Ontario should not use wireless video surveillance cameras without strong security and privacy precautions. Any organization that chooses to use wireless communication technology to transmit personally identifiable information needs to take appropriate proactive measures to protect the privacy of individuals.

What is wireless video surveillance technology?

Wireless video surveillance systems, or wireless CCTV, typically refer to systems that transmit wireless signals to television monitors, not computer screens. The most common commercial use of this equipment is for building security. Commercially available systems do not normally have privacy or security designed into the transmission of the signal. As a result, such systems are easy to install but will allow unauthorized access unless special precautions are taken. Health information custodians must ensure that no one other than specifically authorized staff have the capability of viewing patient images.

www.ipc.on.ca/images/Resources/up-fact_13_e.pdf

Fact Sheet

Wireless Communication Technologies: Safeguarding Privacy & Security

- A good starting point for understanding the impact of technological change is to regularly re-examine past assumptions and decisions;
- Any time wireless technology is used to transmit personal information, that information must be strongly protected to guard against unauthorized access to the contents of the signal.

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

Fact Sheet

Number 14
August 2007

Wireless Communication Technologies: Safeguarding Privacy & Security

We are fast approaching the point where it is reasonable to assume that any device that creates or stores data either has, or is connected to, some form of embedded wireless capability. Cell phones and personal digital assistants (PDAs) are increasingly sophisticated, often combining multiple wireless technologies in a single device.

Wireless technologies can reduce costs, increase efficiencies, and make important information more readily and widely available. In the health care sector, for example, wireless data communications now make it possible for paramedics to send cardiac images and data directly to cardiologists, significantly reducing wait time to treatment.

Clearly, the benefits of wireless communications are many. But, there are also risks. Without appropriate safeguards, transmitting data wirelessly can be like using an open filing cabinet in a waiting room. In fact, this Office just recently issued an Order about a case where unauthorized viewers had inadvertently intercepted wireless video images of patients in a washroom providing urine samples.

This Fact Sheet addresses privacy issues arising from the use of wireless technologies, expanding on Fact Sheet #13, *Wireless Communication Technologies: Video Surveillance Systems*.

Taking Care

The *Personal Health Information Protection Act* (PHIPA), the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) set out requirements for the protection of personal information, including information in electronic form.

In general, compliance with these *Acts* requires that those responsible take reasonable measures to protect personal information, which may include physical safeguards, using role-based access to personal information, or technological measures such as encryption.

The transmission of personal information in electronic form, particularly through the use of wireless technologies, means adding "data-in-motion" to "data-at-rest" as a category of data to protect, and adds another layer of complexity to compliance with these *Acts*.

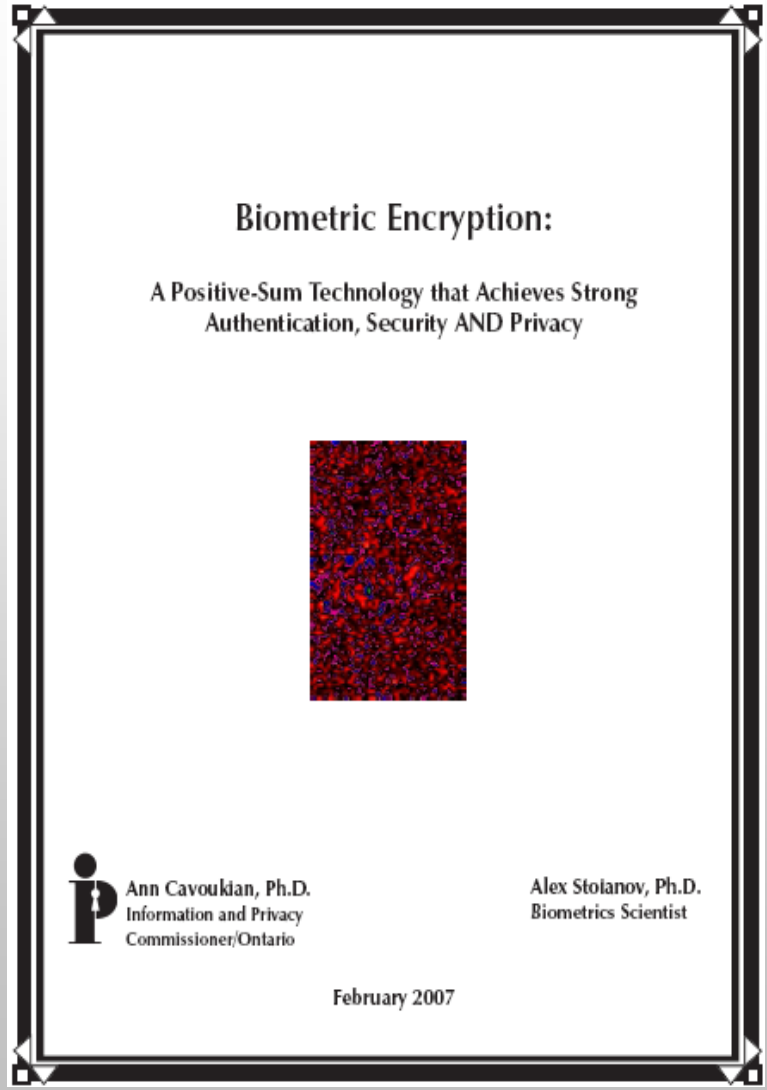
A good starting point for understanding the impact of technological change or new developments is to regularly re-examine past assumptions and decisions. A reasonable precaution is one that any prudent and privacy conscious individual or institution would take. For example, there was a time when it was reasonable to browse the web and download files without

www.ipc.on.ca/index.asp?navid=46&fid1=645

Biometric Encryption

IPC Biometric Encryption Paper

- This paper discusses privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE) – while engaging a broad audience to consider the merits of the BE approach to verifying identity, protecting privacy, and ensuring security;
- The central message is that BE technology can help to overcome the prevailing "zero-sum" mentality by adding privacy to identification and information systems resulting in a "positive-sum," win/win scenario for all stakeholders involved.



www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

Current BE Projects

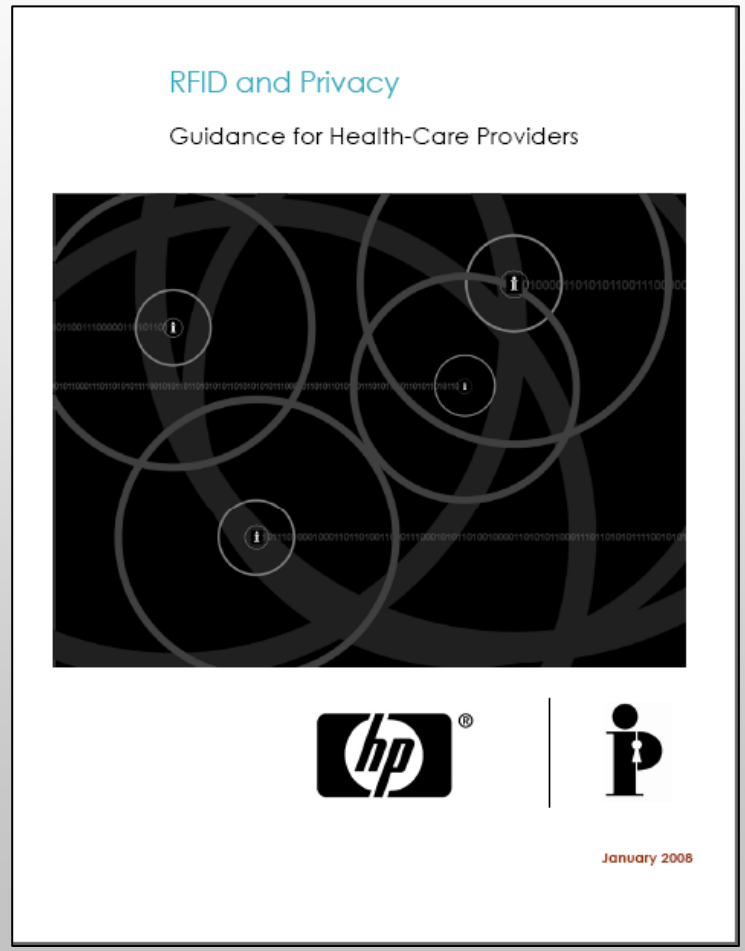
- The **Philips privID™** (Netherlands) is currently one of the most advanced BE technologies in operation; unlike some BE systems, the privID™ system is very fast which allows for a true one-to-many mode; it is also very secure, making it extremely difficult to crack;
- **Bell Canada** is deploying a voluntary voice identity verification service for its customers using technology by biometric vendor **PerSay** (Israel); after only 2 months, Philips was able to clearly demonstrate with success the feasibility of integrating their BE technology with PerSay's voice technology;
- The **Ontario Lottery and Gaming Corporation** (OLG) is exploring the use of facial biometrics to assist Ontarians who voluntarily choose, under the self-exclusion program, to provide photos of themselves so that they can be denied entry into casinos because of their gambling addiction.

RFID

Radio Frequency Identification

RFID and Privacy in Health Care:
Guidance for Health Care Providers

- This paper is organized into three broad categories according to the increasing level of potential risk to privacy:
- RFID technology to track things alone;
- RFID technology to track things associated with people; and
- RFID technology to track people.



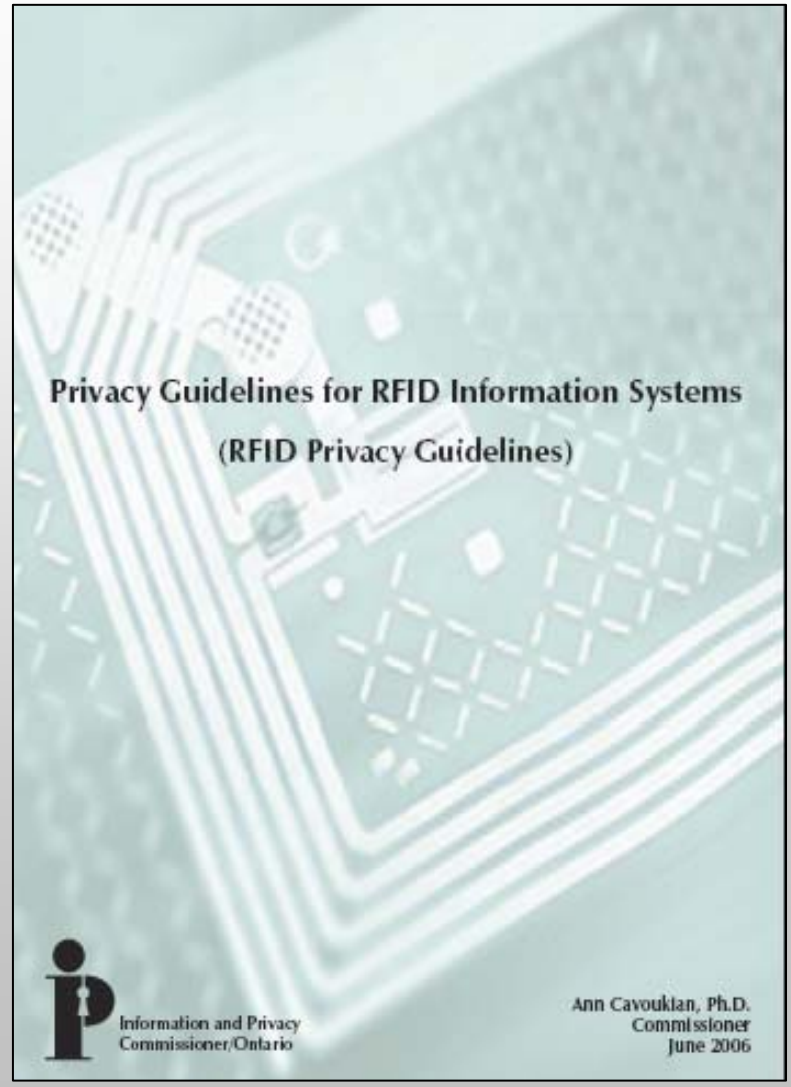
www.ipc.on.ca/images/Resources/up-1rfid_HealthCare.pdf

IPC RFID Privacy Guidelines

The purpose of the *Guidelines* is to promote the embedding of privacy laws into RFID technology by addressing concerns about the potential threat to privacy and to build-in the necessary protections for the item-level use of RFID tags by retailers;

Based on three principles:

1. Focus on RFID information systems, not technologies;
2. Build in privacy and security from the outset, at the design stage;
3. Maximize individual participation and consent.



www.ipc.on.ca/docs/rfidgdlines.pdf

Enhanced Driver's Licenses

Enhanced Driver's Licenses

- **February 2008** – Canada's privacy commissioners issued a joint resolution outlining the steps that need to be taken to ensure the privacy and security of any Canadian's personal information accessed as part of an Enhanced Driver's License (EDL) programs;
- This resolution was in response to the US government encouraging the development of alternative requirements in order to prove identity and citizenship, as part of the implementation of the Western Hemisphere Travel Initiative (WHTI);
- In the joint resolution, I stated that *"I urge the Government of Canada to securely provide citizenship information, upon request, to a province or territory for the purposes of an EDL program, and thus avoid the costs of a cumbersome and highly duplicative process being imposed upon the provinces and territories."*

Joint Resolution on Enhanced Driver's Licenses

- No EDL project should proceed on a permanent basis unless the personal information of participating drivers remains in Canada;
- There must be meaningful and independent oversight of how the U.S. Customs and Border Patrol receives and uses the personal information of Canadians;
- This must include regular reporting of oversight activities and corrective measures to the Government of Canada and to the Privacy Commissioner of Canada.

To see the Joint Resolution in full, visit:
www.ipc.on.ca/images/Resources/Joint%20NR-EDL%20Resolution%20(5Feb08).pdf

RFID Tags in Enhanced Driver's Licenses

- Potential threats to privacy embodied by RFID technology in EDLs:
  - Permit the surreptitious location tracking of individuals carrying an EDL; and
  - Lack of encryption or protection of the unique identifying number assigned to the holder of the EDL and potential unauthorized exposure of any other personal information stored on the RFID.

Response of Joint Resolution to RFID Tags in EDLs

- With regards to RFID tags in EDLs, the Joint Resolution called on the Government of Canada and participating provinces and territories to take steps to ensure the security of personal information stored on the RFID tags embedded in enhanced driver's licences by ensuring that:
  - Robust privacy and security are built into all aspects of EDL projects, by conducting thorough privacy impact assessments and threat risk assessments at the outset;
  - Their EDL programs comply with applicable local privacy legislation; and
  - They consult early and meaningfully with their privacy commissioner or other responsible privacy oversight official on all aspects of any contemplated EDL program.

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