Make Privacy & Security Work *Together* in a Positive Sum Paradigm: *Critical Paths for 2008*

Dr. Ann Cavoukian
Information and Privacy Commissioner
Ontario

CIO Executive Summit
Vancouver, B.C.
February 20, 2008

IPC

Presentation Outline

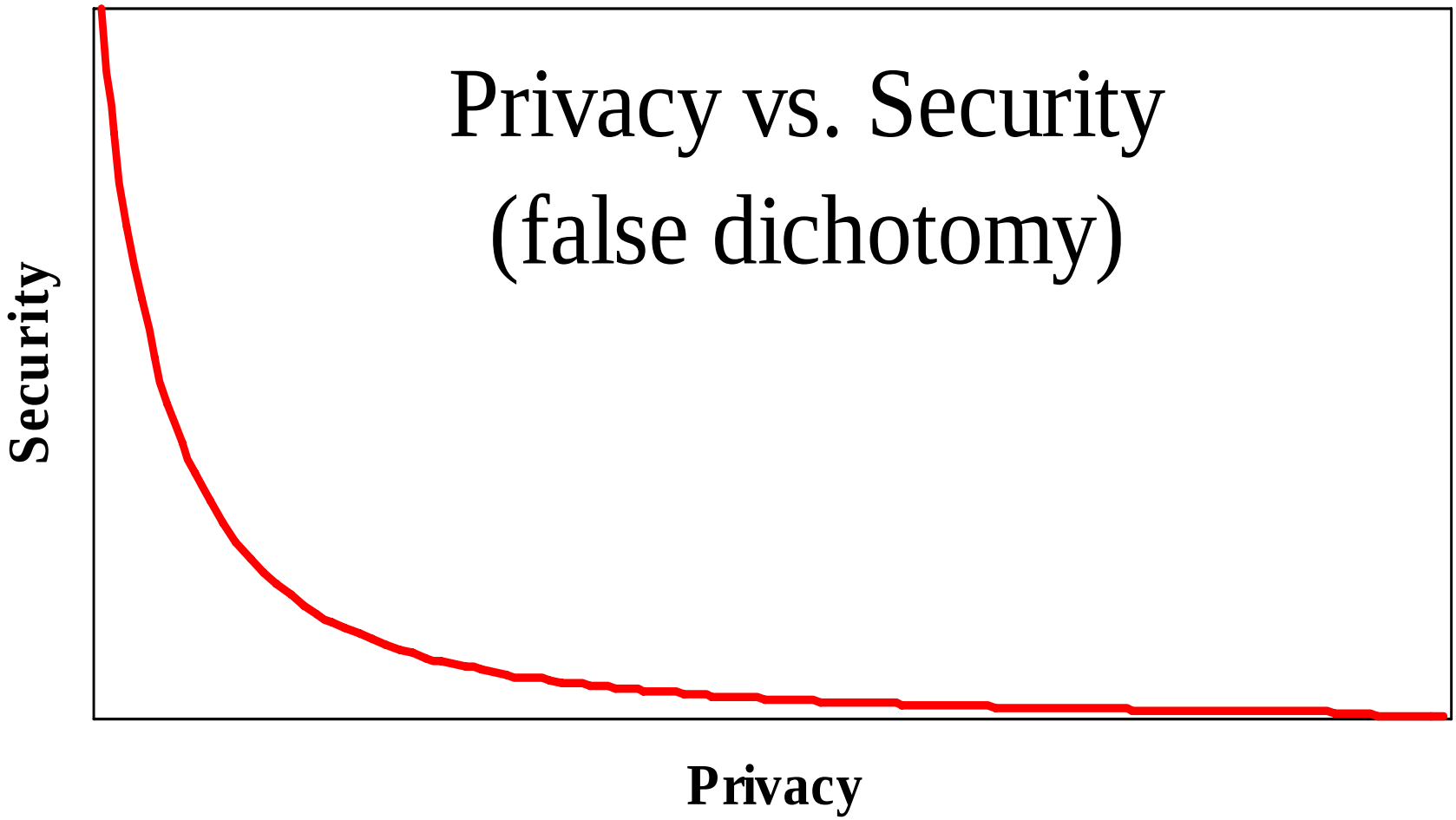
1. *Privacy "101" – Setting the Stage*
2. *Privacy, Security: Not A Zero-Sum Game*
3. *Why Privacy is Good for Business*
4. *Privacy and Technology*
5. *IPC Technology-Related Orders*
6. *Developing A Culture of Privacy*
7. *Conclusions*

IPC

Privacy "101"
Setting the Stage

IPC

Privacy OR Security:
A Zero-Sum Game



IPC

Positive-Sum Model

Change the paradigm

from a zero-sum to

a positive-sum model:

Create a “win-win” scenario

What Privacy is Not

Privacy ≠ Security

Privacy and Security:
The Difference

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation

Security:

Organizational control of information through information systems

- Privacy; Data Protection
- Fair Information Practices
- “Use” of Personally Identifiable Information (PII)

IPC

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."

Fair Information Practices:
A Brief History

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980);
- European Union Directive on Data Protection (1995/1998);
- CSA Model Code for the Protection of Personal Information (1996);
- United States Safe Harbor Agreement (2000);
- Global Privacy Standard (2006).

The Golden Rules:
Fair Information Practices

- **Why are you asking?**
  - Collection; purpose specification;
- **How will the information be used?**
  - Primary purpose; use limitation;
- **Any additional secondary uses?**
  - Notice and consent; prohibition against unauthorized disclosure;
- **Who will be able to see my information?**
  - Restricted access from unauthorized third parties.

Global Privacy Standard

- In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners convened for the sole purpose of creating a single Global Privacy Standard (GPS);
- Globalization and converging business practices created a need to harmonize various sets of fair information practices so that businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems were actually enhancing privacy;
- The GPS builds upon the strengths of existing codes containing time-honoured privacy principles and reflects an enhancement by explicitly recognizing the concept of “data minimization” under the “collection limitation” principle;
- The final version of the GPS was formally tabled and accepted in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

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

Why Privacy is Good for Business

IPC

The Bottom Line

Privacy should be viewed as a **business** issue, not a ***compliance*** issue

CMO Council Study:

Consumer Concerns over Information Security

According to the *Secure the Trust of Your Brand* survey released by the Chief Marketing Officer Council:

- More than **50%** of survey respondents (consumers) said their security concerns were rising;
- **40%** have actually stopped a transaction online, on the phone or in a store due to a security concern;
- More than **30%** indicated they would strongly consider taking their business elsewhere if their personal information was compromised;
- **25%** firmly said they would definitely take their business elsewhere.

— Chief Marketing Officer Council,
Secure the Trust of Your Brand, August 2006. www.cmocouncil.org

IPC

Costs of A Privacy Breach

- Legal liabilities, class action suits;
- Loss of client confidentiality and trust;
- Diminution of brand and reputation;
- Loss of customers, competitive edge;
- Penalties and fines levied;
- Costs of crisis management, damage control, review and retrofit of information systems, policies and procedures.

Privacy Concerns are Adversely Affecting E-Commerce

United States: e-commerce sales were only **2.8%** of total sales -- $108.3 billion in 2006.

— U.S. Dept. of Commerce Census Bureau, February 2007

Canada: Online sales were just over **1%** of total revenues -- $49.9 billion in 2006.

— Statistics Canada, April 2007

IPC

Privacy and Technology

IPC

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.

IPC

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.

Benefits of PETs

- Data protection, such as encryption, is markedly less expensive than cleaning up after a data breach;
- Research has shown that it would cost about $6 per customer account to encrypt data;

— Avivah Litan, Gartner Analyst

- The cost of a breach is much higher – ***30 times higher***;
- In 2006, the average number of records compromised in a corporate privacy breach was about 25,000;
- At an average cost of $182 per record, this meant that each privacy breach incident cost $4.7 million;

— Ponemon Institute

- 100,000 records encrypted = $600,000 vs.
  100,000 records breached = $18,200,000
  — ***You do the math.***

www.ponemon.org/press/Ponemon_2006%20Data%20Breach%20Cost_FINAL.pdf

IPC

Recent IPC Publications on Privacy, Security and Technology

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

Developed with chief scientist, Alex Stoinov, Ph.D., this paper discusses the merits of the biometric encryption approach to verifying identity, ensuring strong security, and protecting privacy;
www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

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

Developed in collaboration with Hewlett Packard (HP) Canada, this joint paper examines a wide variety of RFID applications for the health-care sector, organizing them 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

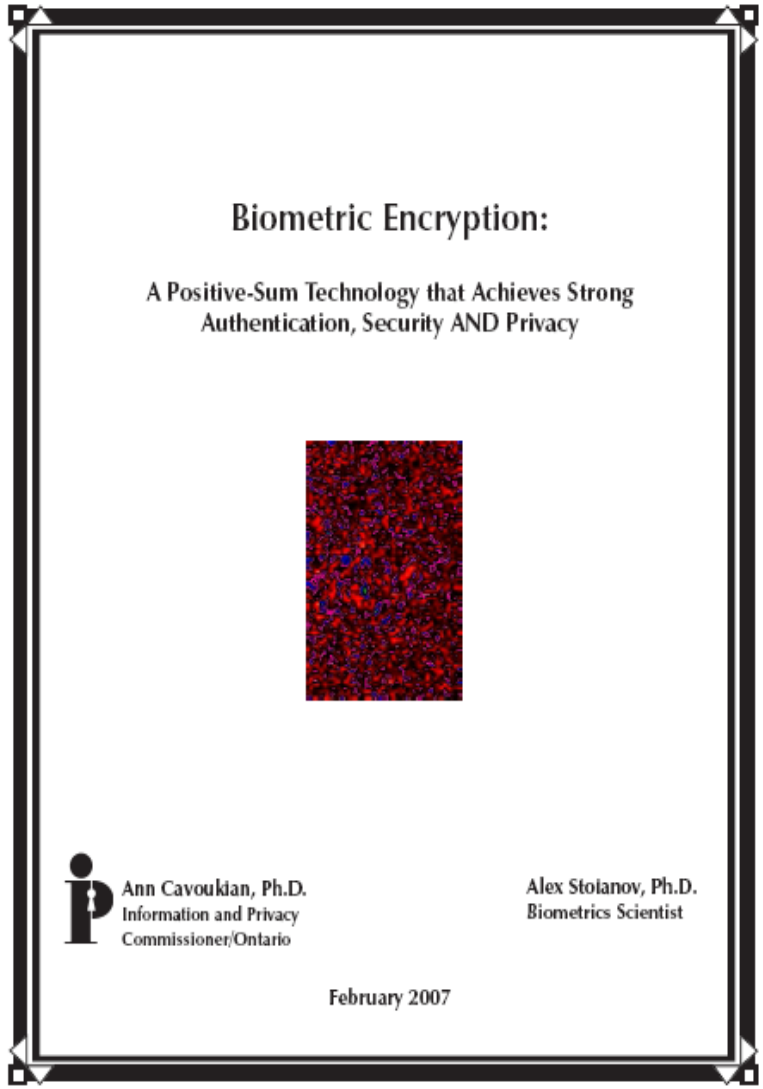
RFID Privacy Guidelines

Developed with EPCglobal Canada, this publication is the strongest, most complete set of RFID guidelines developed to date, and promotes compliance with Canadian federal and provincial privacy laws;
www.ipc.on.ca/docs/rfidgdlines.pdf

IPC Biometrics White 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

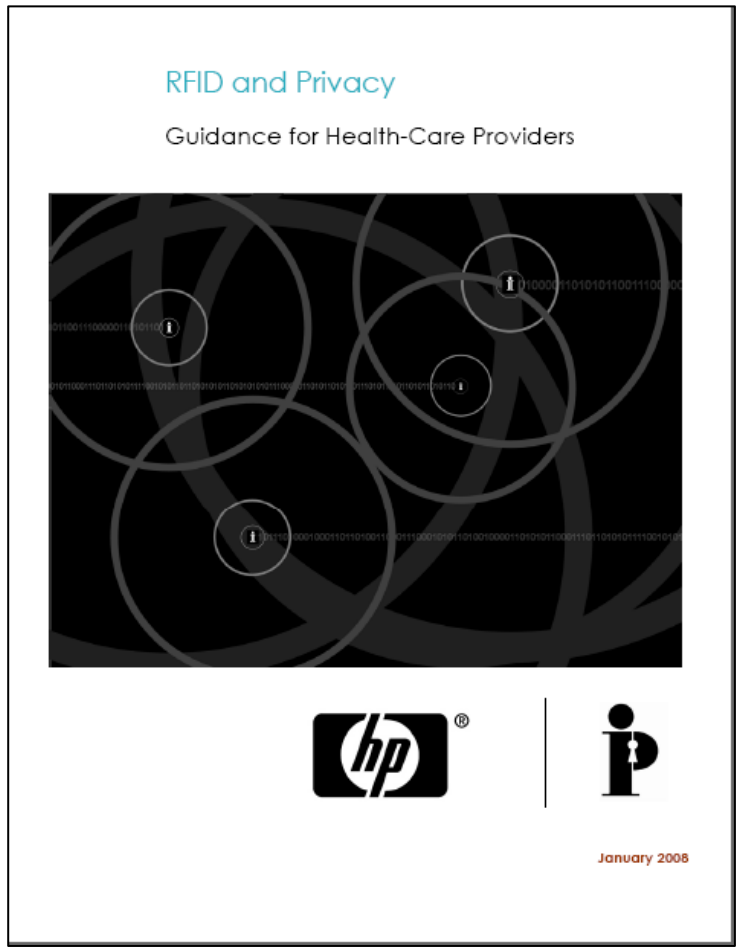
IPC

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;
- 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;
- **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.

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

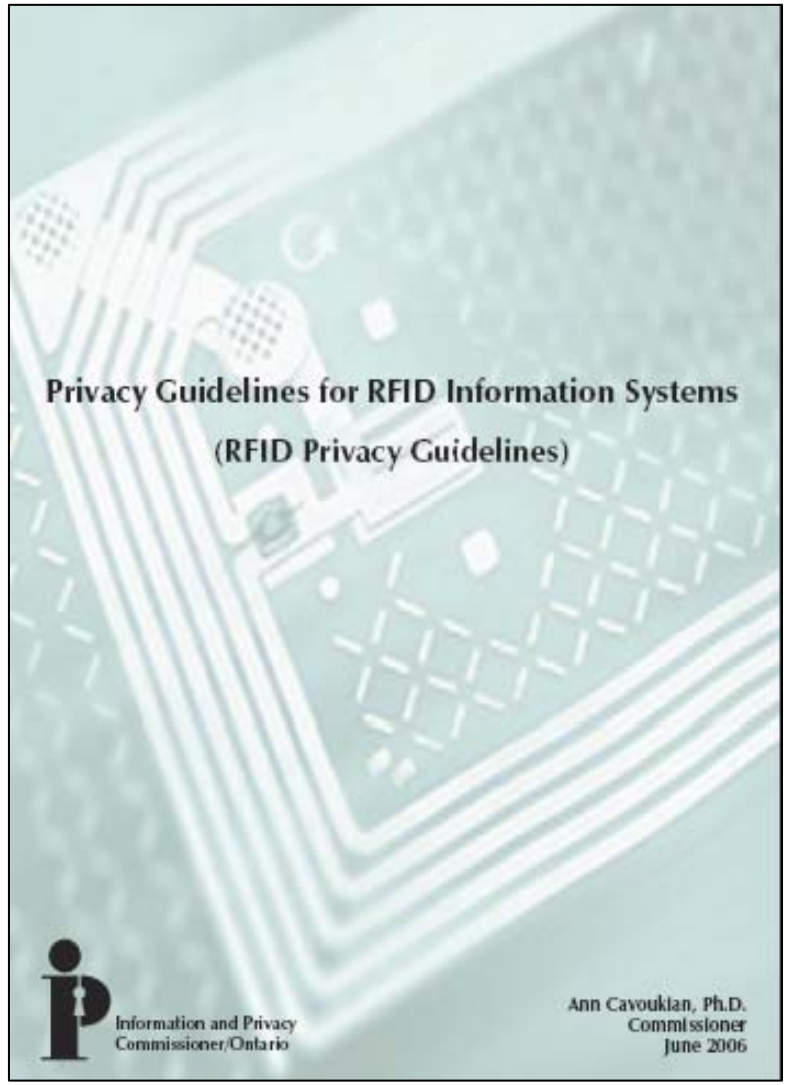
IPC

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

IPC

Biometric Encryption

IPC

Privacy and Biometrics

Issues

- Expanded surveillance;
- Diminished oversight;
- Absence of knowledge or consent;
- Loss of personal control;
- Loss of Use Limitation Principle (Function Creep).

IPC

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;
- A biometric can be used to uniquely encrypt an alphanumeric (AN) and only store the encrypted AN;
- Since the biometric is used to encrypt different ANs for each application, no single template of the biometric is generated or retained in a database (no templates are retained in the system);
- Each biometrically encrypted AN at various applications is completely different, thereby being incapable of being linked together or matched, which completely frustrates the goal of tracking one’s activities.

University of Toronto and the Ontario Lottery Gaming Corporation *Self-Exclusion Program*

- The **Ontario Lottery and Gaming Corporation (OLG)** is exploring the use of facial biometrics to assist Ontarians who voluntarily choose to provide photos of themselves so that they can be denied entry into casinos because of gambling addiction;
- The **University of Toronto** is conducting research to develop a "made in Ontario" BE solution that can be integrated with facial recognition technology;
- In undertaking the research on facial recognition technology, OLG has agreed that the application of BE to the solution they choose will be a win-win not, just for the self-identified gamblers, but also to ensure the privacy of all casino patrons.

IPC

University of Toronto

Privacy-Protected Video Surveillance

- University of Toronto research engineers, Karl Martin and Professor Kostas Plataniotis, have completed research on an innovative technology to protect the privacy of individuals appearing in video and still images. This technology research makes it easy to find and then eliminate personally identifiable images (such as faces) while maintaining the remaining background;
- This method uses a secure object-based coding method whereby objects of interest, such as faces, are stored as completely separate entities from the background surveillance frame and efficiently encrypted and decrypted as necessary. The images can be monitored while still protecting the privacy of individuals;
- As Chair of the University of Toronto's Identity, Security and Privacy Initiative (IPSI), I have been working with the University to advance this privacy-enhancing technology research and we are exploring the possibility of a pilot project involving a large Canadian public transit system.

IPC

IPC Technology-Related Orders

IPC

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.

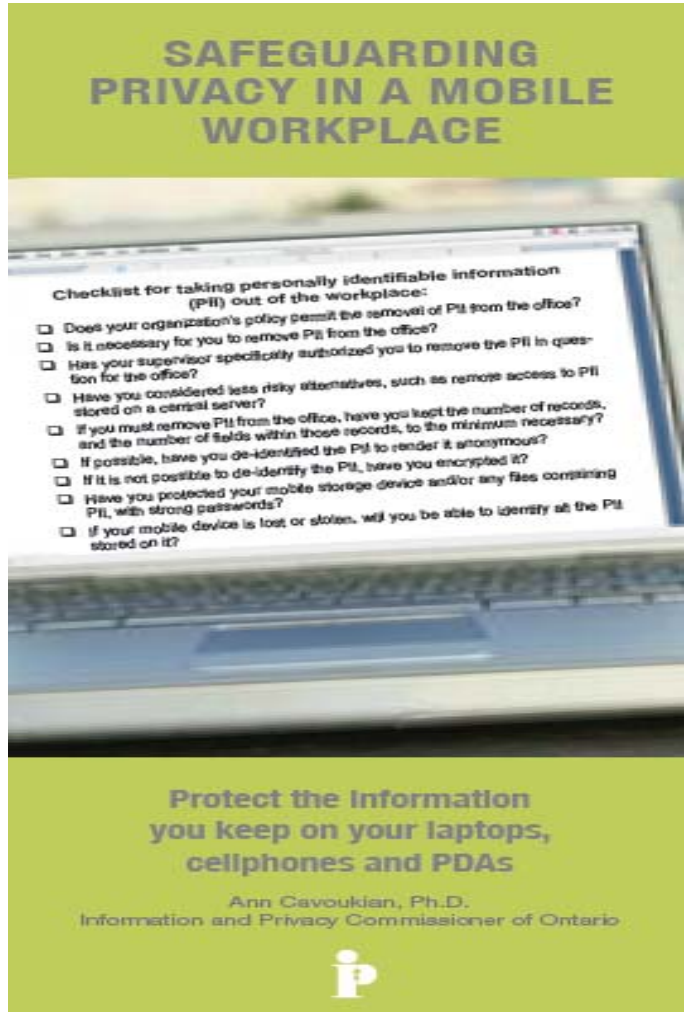
Health Order No. 4
Stolen Laptop Results in Order

- **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

IPC

Health Order No. 5

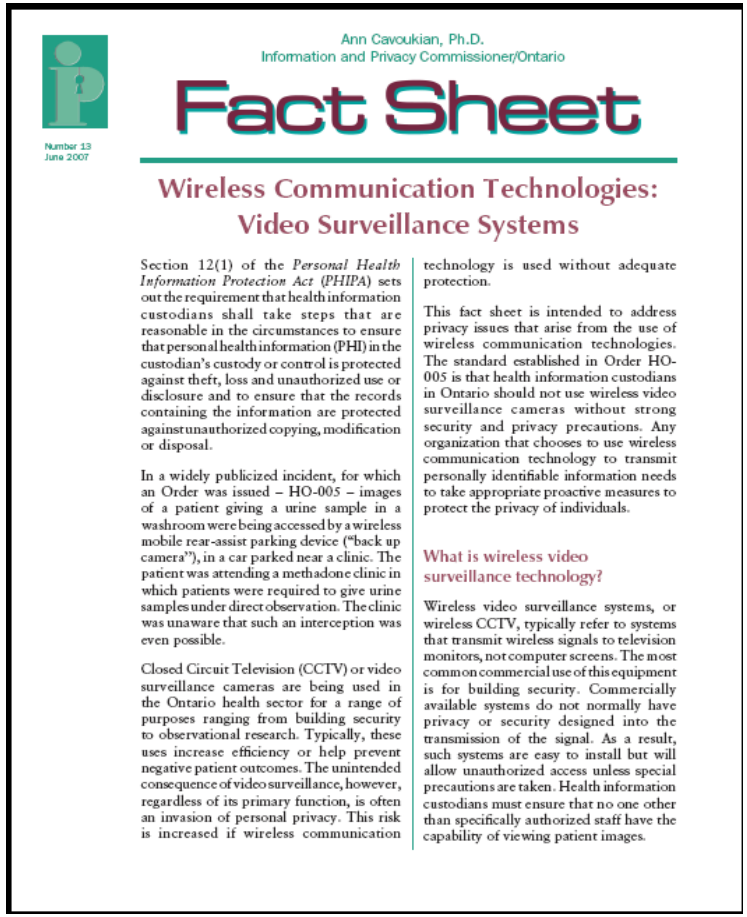
Wireless Technology Results in Order

- **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

IPC

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

IPC

Developing A Culture of Privacy

IPC

Building A Culture of Privacy

- A culture of privacy enables sustained collective action by providing people with a similarity of approach, outlook, and priorities;
- ***The critical importance of privacy must be a message that comes straight from the top;***
- Privacy must be woven into the fabric of the day-to-day operations of an organization, with adequate resources.

Benefits of A Commitment to Privacy

- Strong organizational image and reputation as a leader;
- Enhanced data quality and integrity;
- Savings in terms of time and money (e.g., avoid lawsuits, avoid requirement to notify individuals following a privacy breach, etc.).

Weaving Privacy into Your Day-to-Day Operations

- On-going privacy training and awareness program (new staff training; refresher training for existing staff, new threats to privacy, new technology threats and solutions);
- Policies and procedures for maintaining privacy must be clearly articulated and individuals must know how to apply them in the day-to-day work;
- Privacy must form part of the performance standard for every individual working with personally identifiable information.

Conclusions

- Privacy principles are embodied in “Fair Information Practices;”
- Privacy does ***not*** equal Security – you need both;
- Privacy does ***not*** have to be sacrificed for Security – that is a false dichotomy; Change the paradigm from a zero-sum to a positive-sum model: Create a “win-win” scenario;
- Privacy by Design: Build it in – bake it right into the technology;
- Privacy should be viewed as a business issue, not a compliance issue;
- Build a “culture of privacy”: Weave privacy right into the fabric of the day-to-day operations of your organization;
- The critical importance of privacy must be a message that comes straight from the top;
- Privacy is good for business: Build it in and gain a sustainable competitive advantage.

IPC

How to Contact Us

Ann Cavoukian, Ph.D.

Information and 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