

“Privacy by Design”

A Crucial Design Principle

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner of Ontario
Chair, Advisory Council, IPSI**

**Identity, Privacy and Security Initiative
University of Toronto
*September 17, 2007***



Presentation Outline

- 1. Privacy “101” – Setting the Stage*
- 2. Privacy-Enhancing Technologies (PETs)*
- 3. Privacy By Design: “Build It In”*
- 4. Technology-Related Applications*
- 5. Biometrics and Privacy*
- 6. Biometric Encryption*
- 7. Conclusions*



Privacy “101”

Setting the Stage



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.”



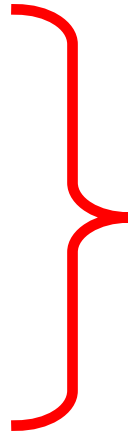
What Privacy is Not

Privacy \neq Security



Privacy and Security: *The Difference*

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation



Security:

Organizational
control of information
through information
systems, networks

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



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).



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.



Fair Information Practices:

The Golden Rules

- **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?**
 - Restrict access to unauthorized third parties.



Privacy Laws

Canada, United States, Europe and Asia

Canada:

- Public sector privacy laws: federal, provincial and municipal;
- Private sector privacy laws: (Federal) *Personal Information Protection and Electronic Documents Act (PIPEDA)*;
- Provincial: Quebec, British Columbia, Alberta, Ontario;

United States:

- Federal public sector *Privacy Act*;
- Sectoral privacy laws;
- Safe Harbor Agreement;

Europe:

- Both private and public sector privacy laws;
- European Directive on Data Protection;

APEC (Asia-Pacific Economic Cooperation):

- Mixture of public and private-sector laws.



Global Privacy Standard:

Privacy Principles

- 1. Consent**
- 2. Accountability**
- 3. Purposes**
- 4. Collection Limitation – Data Minimization**
- 5. Use, Retention, Disclosure Limitation**
- 6. Accuracy**
- 7. Security**
- 8. Openness**
- 9. Access**
- 10. Compliance**



Data Minimization Principle

Global Privacy Standard

Privacy Principle # 4

Collection Limitation: The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

Data Minimization: The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions **as the default**. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.



Use Limitation Principle

Global Privacy Standard

Privacy Principle # 5

Use, Retention, and Disclosure Limitation:

Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.



Privacy-Enhancing Technologies (PETs)



Privacy-Enhancing Technologies (*PETs*)

- The IPC coined 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).



Privacy-Enhancing Technologies (*PETs*)

- Privacy Enhancing Technologies enlist the support of technology to **protect** privacy. They include those that empower individuals to manage their own identities and personally-identifiable information (PII) in a privacy enhancing manner – encryption plays a key role.
- 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 PII to others and exert maximum control over their PII once disclosed.



Privacy By Design: *“Build it In”*



Technology Is Essential

- “The most effective means to counter technology’s erosion of privacy is technology itself.”

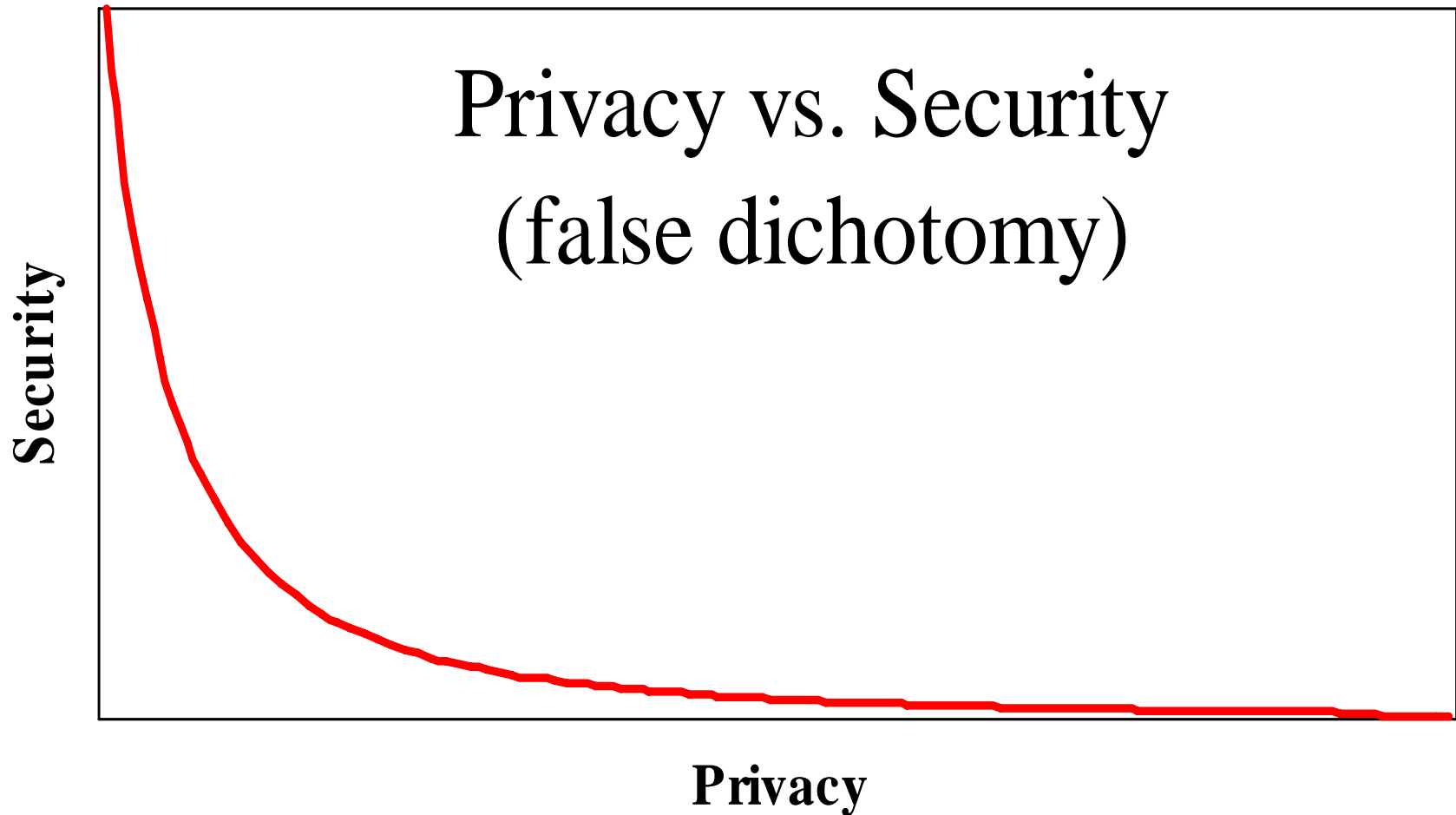
— Alan Greenspan, Federal Reserve Chairman, 2000.

- “A technology should reveal no more information than is necessary...it should be built to be the least revealing system possible.”

— Dr. Lawrence Lessig, Harvard, 1999.



Prevailing (Dark Ages) Model: *Privacy vs. Security: A Zero-Sum Game*





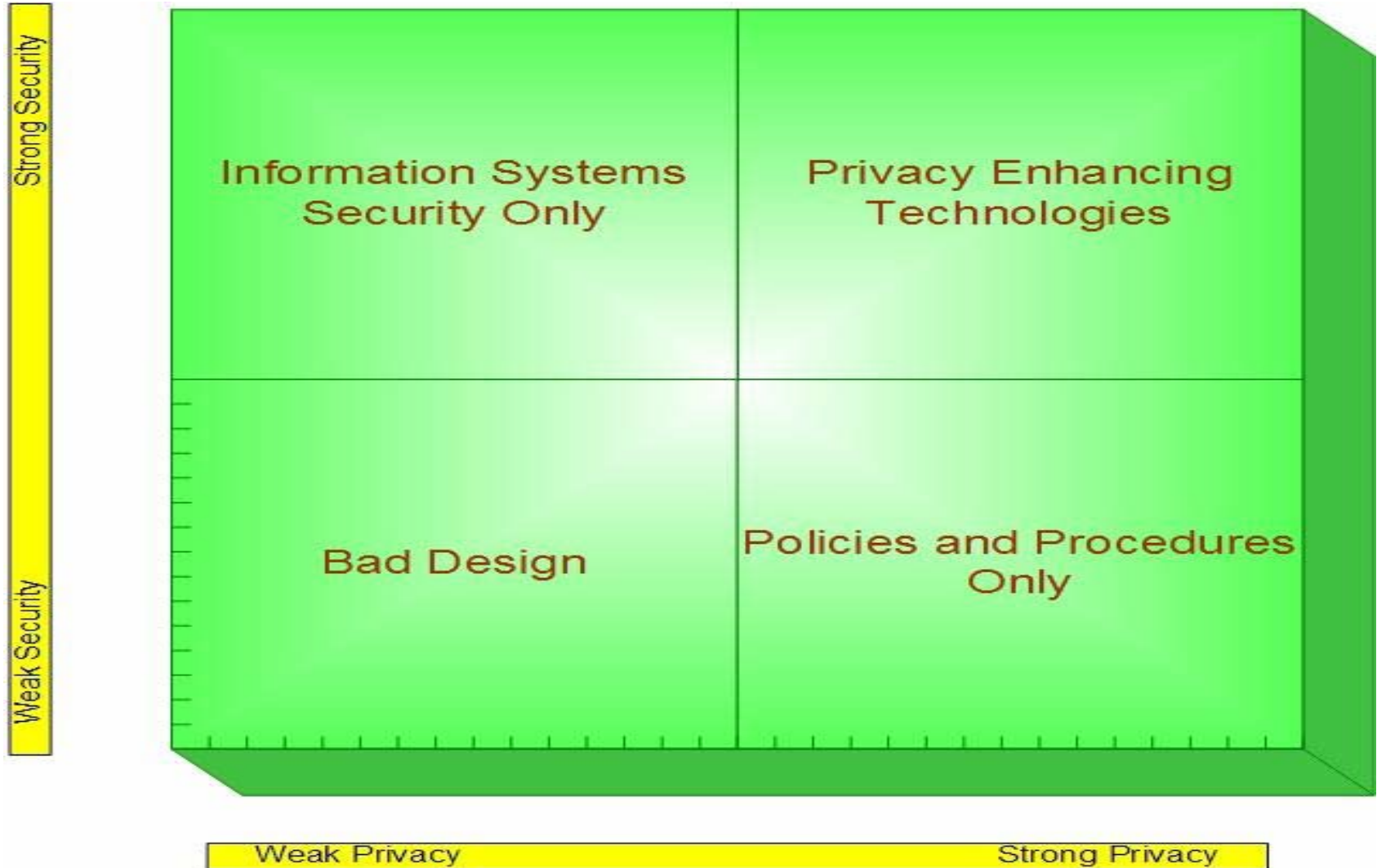
Emerging (Progressive) Model: *Positive-Sum Paradigm*

*Change the paradigm
from a zero-sum to
a positive-sum model*



Privacy AND Security

(Privacy by Design)





Privacy By Design

Convergence of Privacy and Security (A Positive-Sum Model)

- **Data minimization is key:** minimize the routine collection and use of personal information;
- Use encrypted or coded information whenever possible – encrypt personally identifiable information;
- Build in privacy – up front, right into the design specifications – become a privacy architect;
- Assess the risks to both privacy and security: conduct an *information* impact assessment.



Encryption:

The Original PET

- Encryption involves a process of converting ordinary “plaintext” into random “ciphertext;”
- Encryption (decryption) enabled by users’ secret keys;
- Ensures confidentiality (and integrity) of data at rest and in motion;
- Security is a function of the strength of encryption algorithms and the secrecy of the keys used;
- **Single key** (symmetric) and **public key** (asymmetric) cryptosystems;
- Astonishingly diverse range of uses and applications.



IPC and Encryption

- IPC has a long history of advocating use of encryption:
 - Preventing data breaches (identity theft) from lost or stolen hard drives, backup tapes, etc.;
 - Securing data on laptops, PDAs, and other mobile devices;
 - Securing wireless routers, communications and video signals;
 - Authenticating the identities of remote users;
 - Electronic Messaging, attachments, and other e-communications;
- Advocate of innovative privacy-enhanced encryption methods:
 - Biometric Encryption;
 - IBM's IDEMIX™ – anonymous credential system;
 - CREDENTIALICA's U-Prove™ – software development toolkit for user-centric identity and access management;
 - Privacy-enhanced data-matching (via cryptographic hashing).



Technology-Related Applications



Technology-Related Applications

- Mobile devices;
- Wireless technologies;
- Radio Frequency Identifiers (RFIDs);
- Internet design principles:
The 7 Laws of Identity;
- Biometric Encryption.



Mobile Devices

- According to a 2006 survey conducted by the Ponemon Institute, **81%** of companies surveyed reported the loss of one or more mobile devices containing sensitive information;
- One of the main reasons corporate data security breaches occur is because companies don't know where their confidential business information resides within the network or enterprise systems;
- PDAs, laptops and memory sticks posed the greatest security risk for sensitive corporate data;
- Approximately **50%** of respondents reported that their companies would not be able to determine what confidential information resided on a lost or stolen PDA, laptop or memory stick.

— Linda Rosencrance,

Survey: 81% of U.S. firms lost laptops with sensitive data in the past year,
ComputerWorld, August 16, 2006.



IPC Health Order No. 4

Stolen Laptop Results in Order

- Despite the known high risks of loss or theft, personal health information was transported out of a hospital on a portable device (a laptop) by a physician, without safeguards;
- The Hospital was ordered to either de-identify or encrypt **all** personal health information before allowing it to be removed from the workplace;
- **Health Order No. 4** (HO-04) created the standard of practice expected regarding the removal of identifiable health information from a healthcare facility – **if it's not encrypted, it's not in compliance** with *PHIPA*.



Encrypting Personal Health Information on Mobile Devices

- Why are login passwords not enough?
- What is encryption?
- What are the options?
 - Whole disk (drive) encryption
 - Virtual disk encryption
 - Folder or Directory encryption
 - Device encryption
 - Enterprise encryption



Number 12
May 2007

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

Fact Sheet

Encrypting Personal Health Information on Mobile Devices

Section 12 (1) of the *Personal Health Information Protection Act, 2004 (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.

The Office of the Information and Privacy Commissioner/Ontario recognizes that the delivery of health care may require the use of PHI outside of the workplace, and that such PHI may most effectively be transported and used in electronic form. Notwithstanding the ease of use and portability of electronic documents, it is still important that only the minimum necessary data be transported in this manner.

Because of the high incidence of loss or theft of mobile devices such as laptop computers, personal digital assistants (PDAs), or flash drives, custodians need to ensure that personal health information that is stored on mobile devices is encrypted. When encryption is implemented properly, it renders PHI safe from disclosure. The availability of encryption means that it is easier to safeguard electronic records of PHI than it is to safeguard paper-based records when being transported.

This fact sheet is intended for health information custodians who store PHI on mobile devices. However, it is also relevant to anyone who stores personal information on a mobile device. If you are unsure of the meaning of these guidelines, please consult a computer systems security expert to determine how to apply this fact sheet to the information in your care. In many cases, encryption can be as easy as installing a simple program and implementing proper key management for the system.

Why are login passwords not enough?

It is not acceptable to rely solely on login passwords to protect PHI on devices that are easily stolen or lost. 'Strong' login passwords will prevent casual access to data on a device, but may not prevent access by knowledgeable thieves. Strong login passwords are usually characterized by:

- No dictionary words;
- A combination of letters, numbers and symbols;
- Eight or more characters, with 14 or more being ideal.

For example, "LetMeIn" is a weak password because it uses dictionary words. On the other hand, you could remember the phrase, "My birthday is October 21 and I'm 25"

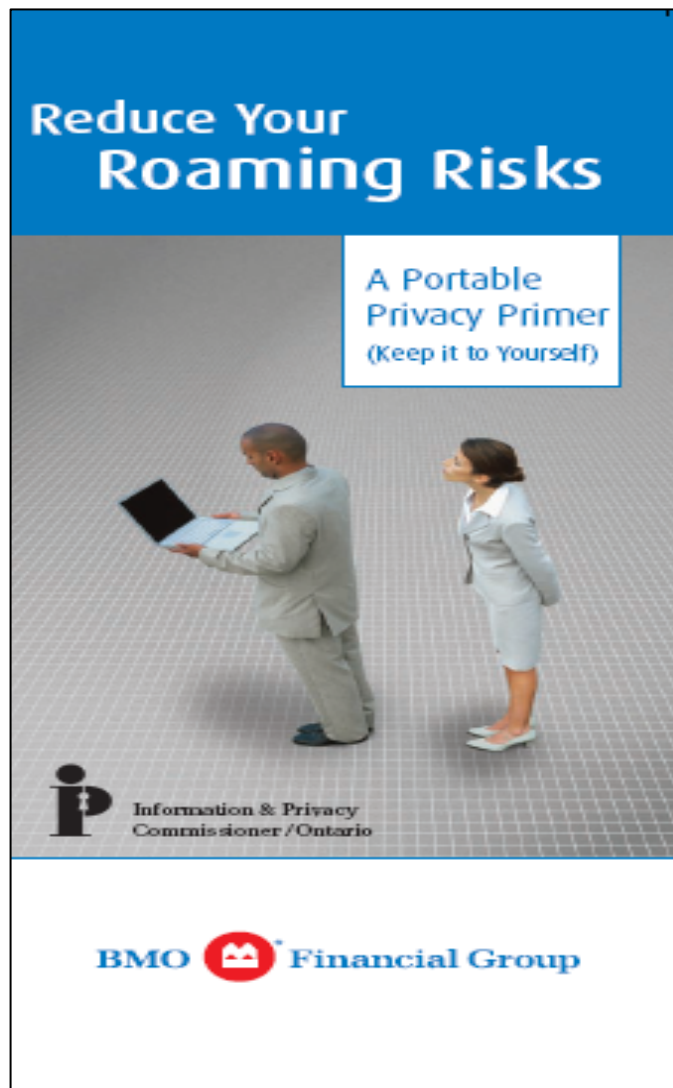


Reduce Your Roaming Risks

A Portable Privacy Primer

IPC-BMO Publication:

- Working away from the “bricks and mortar” office also means working outside the traditional security layers. As a result, appropriate steps need to be taken to safeguard confidential information;
- This brochure outlines some of the risks associated with “mobile” technology (especially while away from the office) and offers advice on how to reduce these risks.





Wireless Communications Technology Used at Methadone Clinic


- **May 2007**, CBC Radio (Sudbury) reported an incident involving a Sudbury methadone clinic which was inadvertently broadcasting video images of patients giving urine samples in the clinic's washroom – *those images could apparently be seen by anyone using basic wireless technology outside of the medical building*;
- My office immediately launched an investigation on the same day and soon afterward, the inadvertent broadcasting was stopped and will not continue;
- I issued Order No. 5 which set a new standard of practice in Ontario: if you use wireless technology, you must encrypt the transmission of all personally identifiable information;
- My office also prepared a Fact Sheet to underscore this privacy principle for everyone who chooses to use wireless technology as part of a health delivery program or information management 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.



Number 13
June 2007

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

Fact Sheet

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.



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.



Number 14
August 2007

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

Fact Sheet

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



Radio Frequency Identifiers (RFIDs)

Privacy Challenges

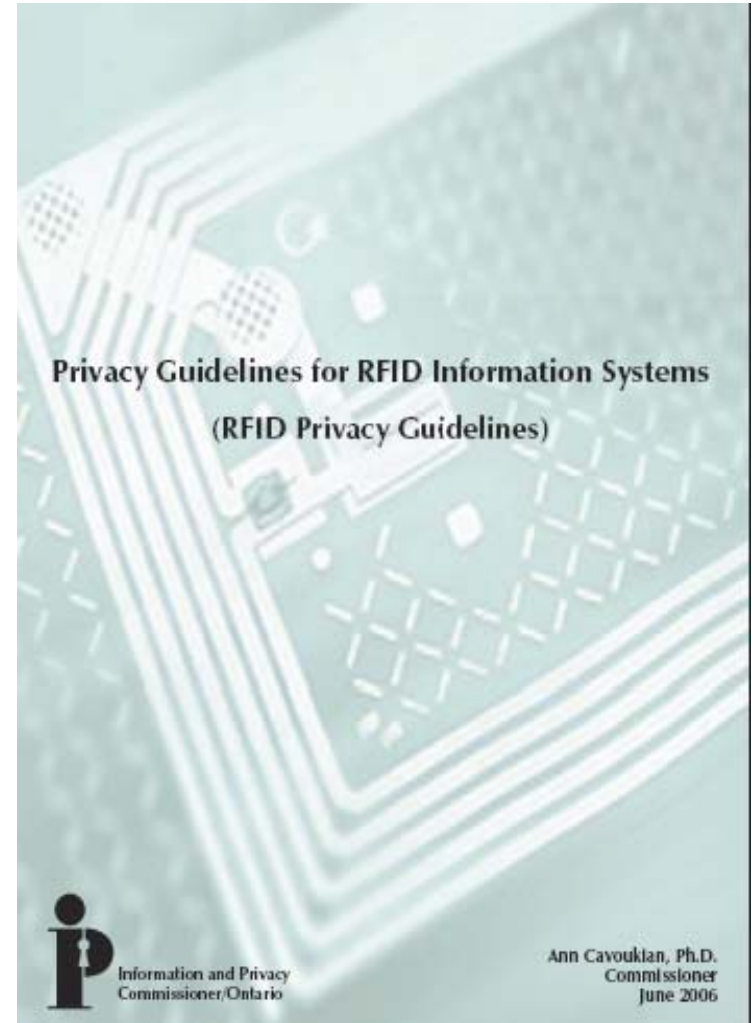
- RFID technologies not well known or understood by public. Public opinion on RFIDs still developing; perceived as a privacy issue: concerns about possible surveillance, secondary uses;
- Privacy issues can arise when the RFID tag is associated with a specific item and an identifiable individual (consumer); but do not arise in the absence of personally identifiable information;
- **Supply-chain management:** involves tagging bulk goods and tracking cases and pallets for back-end retail inventory management purposes; Generally used for inventory control;
- **Item-level consumer product tagging:** involves tagging commercial products in the retail space that are owned, carried and used by individual consumers, such as apparel, electronics, and identity or payment cards.



IPC RFID Privacy Guidelines

- Developed with leading industry standards-setting organization (GS1/EPCglobal Canada);
- Promotes compliance with Canadian federal and provincial privacy laws;
- Strongest, most complete set of RFID guidelines developed to date – promotes compliance and consumer trust.

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





Privacy-Embedded 7 Laws

“The existing identity infrastructure of the Internet is no longer sustainable. The level of fraudulent activity online has grown exponentially over the years and is now threatening to cripple e-commerce. Something must be done now before consumer confidence and trust in online activities are so diminished as to lead to its demise ... Enter the 7 Laws of Identity.”

— *7 Laws Of Identity:
The Case For Privacy-Embedded Laws Of Identity In The Digital Age,*
Information and Privacy Commissioner of Ontario, 2006.



“Privacy-Embedded”

7 Laws of Identity

- An identity metasystem (described by the 7 Laws) is a necessary, but not sufficient, condition for privacy-enhancing options to be developed;
- What was needed was *privacy-enabling* design options for identity systems to be identified and then embedded, thus immersing privacy and data protection into the design;
- The privacy-embedded Identity Metasystem is the result of “mapping” fair information practices over the 7 Laws, to explicitly extract their privacy-protective features;
- The result is a commentary on the 7 Laws that extracts its privacy implications, for all to consider.



“Privacy-Embedded”

7 Laws of Identity

1. Personal Control and Consent:

Technical identity systems must only reveal information identifying a user with the user’s consent;

2. Minimal Disclosure For Limited Use: Data Minimization

The Identity Metasystem must disclose the least identifying information possible. This is the most stable, long-term solution. It is also the most privacy protective solution;

3. Justifiable Parties: “Need To Know” Access

Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship;



“Privacy-Embedded”

7 Laws of Identity (Cont’d)

4. Directed Identity: Protection and Accountability

A universal Identity Metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy;

5. Pluralism of Operators and Technologies: Minimizing Surveillance

The interoperability of different identity technologies and their providers must be enabled by a universal Identity Metasystem;

6. The Human Face: Understanding Is Key

Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks;

7. Consistent Experience Across Contexts: Enhanced User Empowerment And Control

The unifying Identity Metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.



Implications for Users

The Privacy-Embedded 7 Laws of Identity offer:

- Easier and more direct control over one's personal information when online;
- Embedded ability to minimize the amount of identifying data revealed online;
- Embedded ability to minimize the *linkage* between different identities and online activities;
- Embedded ability to detect fraudulent emails and web sites (less phishing, pharming, fraud).



Biometrics and Privacy



Growth of Biometrics

- **Border Crossings:** Increasingly, countries are considering including biometric border crossing documents;
- Several countries are in the process of developing and implementing programs for biometrically enhanced National ID cards;
- **International Civil Aviation Organization (ICAC)** approved the use of facial recognition for travel documents;
- Biometric technologies are beginning to be utilized in U.S. and U.K. schools for library services, vending machines, class attendance and tuition payments;
- **CANPASS** – Facilitates efficient and secure entry into Canada by allowing pre-approved travelers to meet their border clearance obligations by simply looking into a camera that recognizes the iris of the eye as proof of identity;
- **NEXUS** – A Canadian joint program with U.S. Customs designed to expedite the border clearance process for low risk, pre-approved frequent travelers;
- **EU** to implement biometrics in passports and visas; in the **United States** biometric passports began to be issued in 2006.
- **BioPay LLC** – developing and implementing a biometric payment system for retail stores in the U.S.



European Biometrics Forum

- The European Biometrics Forum (EBF) was launched in 2003 – I was invited to speak at their inaugural conference in Dublin;
- Then asked to become a member of the International Biometrics Advisory Council (IBAC);
- Composed of leading biometrics and technology experts, the EBF was established to develop world-class standards, best practices and innovation in the biometric industry to strengthen trust and confidence in the use of emerging biometric applications;
- The EBF is supported by a network of national biometric organizations, companies, universities and experts across Europe in carrying out research for the development of a roadmap for the European Biometrics industry by 2010.



Privacy and Biometrics:

The Risks

- Creation of large centralized databases containing biometric templates (that may then be linked together) – the potential for surveillance;
- Far-reaching consequences of errors in large-scale networked systems – false positives and false negatives;
- Interoperability that invites additional unintended “secondary” uses (contrary to the Use Limitation Principle).



Privacy and Biometrics

Risks (Cont'd)

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



Biometric Applications

- **Identification:**
 - one-to-many comparison;
- **Authentication/Verification:**
 - one-to-one comparison.



Centralized Databases

- Risks associated with large centralized, networked biometric databases;
- Article 29 Working Group, chaired by Peter Schaar, Germany's federal Data Protection Commissioner,

“Strictly opposes the storage of all EU passport holders’ biometric and other data in a centralized data base.”

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_en.pdf (2004)



Interoperability

- Interoperable biometric databases invite additional purposes and secondary uses of the data;
- E.U. Data Protection Supervisor, Peter Hustinx, in his March 2006 Opinion, stressed that:

“Interoperability of systems must be implemented with due respect for data protection principles and in particular, the use limitation principle.”

Comments on the Communication of the Commission on interoperability of European databases, www.edps.eu.int/legislation/Comments/06-03-10_Comments_interoperability_EN.pdf



1:1 versus 1:Many

- Privacy regulators favor 1:1 authentication (verification) over 1:many identification;
- The EU Article 29 Working Group Resolution on the use of biometrics in passports, identity cards and travel documents was passed by Data Protection and Privacy Commissioners in Montreux, Switzerland, 2005:

“...The Conference calls for the technical restriction of the use of biometrics in passports and identity cards to verification purposes comparing the data in the document with the data provided by the holder, when presenting the document.”

— 27th International Conference of Data Protection and Privacy Commissioners,
Montreux, 16 September 2005

www.privacyconference2005.org/fileadmin/PDF/biometrie_resolution_e.pdf



Authentication/Verification:

Biometric Strength (Security) and Privacy

The strength of one-to-one matches:

- Authentication/verification does not require the central storage of biometric templates;
- Biometric may be stored locally, not centrally – on a smart card, token or travel document, and then compared to the live sample;
- Delivers both security **and** privacy.



Biometric Encryption



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
 - total privacy



Biometric Encryption (Cont'd)

- 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 (there are no templates in the system);
- Thus, the biometric can never serve as a unique identifier – it stays on your finger (or iris), where it belongs;
- The privacy threat of using a biometric for tracking or profiling purposes is eliminated because no biometric or template is stored, whose footprints can be tracked;
- Each biometrically encrypted AN at various applications is completely different, thereby being **incapable** of being linked or matched; this completely frustrates the goal of tracking one's activities.



Unlimited Applications and Uses of Biometric Encryption

- Biometric ticketing for events;
- Biometric boarding cards for air travel;
- Identification, credit and loyalty card systems;
- “Anonymous” (untraceable) labeling of sensitive records (medical, financial);
- Consumer biometric payment systems;
- Access control to personal computing devices;
- Personal encryption products;
- Local or remote authentication to access files held by government and other various organizations.



Advantages of Biometric Encryption

BE Embodies core privacy practices:

- 1. Data minimization:** no retention of biometric images or templates, minimizing potential for unauthorized secondary uses, loss, or misuse;
- 2. Maximum individual control:** Individuals may restrict the use of their biometric data to the purpose intended, thereby avoiding the possibility of secondary uses (function creep);
- 3. Improved security:** authentication, communication and data security are all enhanced.



Philips BE Technology

- The IPC became aware of Philips' BE work in 2006 when we learned of their **privID™** biometric encryption system;
- We met with senior Philips researchers to witness a demo of privID™ and were assured that it was operational;
- The Philips privID™ system 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 difficult, if not impossible, to crack;
- Presently at a prototype stage, Philips is looking forward to a large-scale deployment of its BE technology.



Philips BE Technology and PerSay

Integrating BE with Voice Biometric Technology

- Bell Canada is deploying a voluntary voice identity verification service for its customers using technology by biometric vendor PerSay – as of September 2007, there have been over 325,000 voluntary enrollments;
- We asked the researchers at Philips to work with Bell's **voice** biometrics vendor, PerSay, to see if it would be feasible to integrate BE with PerSay's voice biometrics;
- 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 performance results were surprisingly positive – contrary to what was expected when Philips applied their BE to PerSay's voice technology, the performance of the combined technology remained at a superior level.



Ontario Lottery Gaming Corp.

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 their gambling addiction;
- Any technology solution that the OLG considers will need to be cost-effective, able to detect self-identified gamblers, not interfere with the smooth flow of other patrons into the casino, and respect **all** casino patrons' privacy;
- In undertaking their 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.



University of Toronto and the Ontario Lottery Gaming Corporation

- The University of Toronto has agreed to undertake the necessary research to develop a “made in Ontario” BE solution that can be integrated with facial recognition technology;
- When the lab work is completed over the next few months, we believe this BE solution will lead to a commercially viable product that will garner considerable acclaim for Ontario and Canada;
- The OLG’s support of this BE research and product development is a demonstration of responsible public management with respect to gaming and privacy protection.



Conclusions



Conclusions

- Starting today, engage in a new way of thinking. Start by asking: Is it personal information, meaning is it personally identifiable? If so, then go down the privacy track: Think, “Fair Information Practices” and “Privacy-Enhancing Technologies;”
- Privacy-Enhancing Technologies, “Privacy by Design,” where privacy is architected directly into technology – may be the only way to truly preserve privacy well into future generations;
- We must change the prevailing exclusionary “zero-sum game” paradigm into one of inclusion and convergence – a positive-sum model, that delivers **both** privacy and security;
- Privacy is essential to freedom and liberty. It is an enabling right, forming the foundation for our basic rights and freedoms. Without privacy, freedom disappears.



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