Cracking Down on Unencrypted Mobile Devices: *"Stop. Think. Protect"*

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

SC Congress
DATA SECURITY CONFERENCE & EXPO
Canada 2010

Presentation Outline

1. *Why We Need to Change the Paradigm*
2. *The Future of Privacy: My Prediction*
3. *Privacy by Design: The Gold Standard*
4. *Personal Health Information Protection Act* **(PHIPA)**
5. *Technology-Related Health Orders under PHIPA*
6. *Stop. Think. Protect*
7. *Conclusions*

Setting the Stage:

Why We Need to Change the Paradigm

If Privacy is to Survive, Things Have to Change

The Future of Privacy

Change the Paradigm to Positive-Sum,

NOT

Zero-Sum

Positive-Sum Model

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

The Future of Privacy: My Prediction

My Prediction

"The world has less than a decade to make the protection of personal information and online privacy a priority before the concepts are lost forever … online privacy problems will only worsen if governments don't take a hard stance."

— Commissioner Cavoukian,
Ottawa Citizen, August 18, 2010

World is losing grip on privacy: watchdog

Next decade will be crucial in protecting personal data

BY VITO PILIECI

The world has less than a decade to make the protection of personal information and online privacy a priority before the concepts are lost forever, warns Ontario's information and privacy commissioner.

Ann Cavoukian says legislation meant to safeguard privacy already can't keep pace with the flow of information and advances in technology.

"We have a large job to do," she told about 100 people Tuesday at a conference at the University of Ottawa.

"This is sort of a David vs. Goliath thing."

Cavoukian's call comes as Facebook, Google and other companies have been forced to examine how they handle personal data.

Facebook in particular has been under the microscope of privacy advocates around the world who have criticized the social networking company for sharing too much of the personal information of members with marketing firms.

Google was caught collecting private Wi-Fi data in 30 countries in June. The Internet company, which claims the data collection was unintentional, also has been forced to repeatedly defend its StreetView mapping service, which many complain is too invasive.

BRUNO SCHLUMBERGER, OTTAWA CITIZEN

'It's your information, you should be able to decide what happens to it.'

ANN CAVOUKIAN
Ontario's information and privacy commissioner

Cavoukian said online privacy problems will worsen if governments don't take a hard stance.

Several tools are being used by hackers to steal personal data by tricking consumers into viewing websites infected with worms and viruses, and there are still no laws in place forcing private companies to disclose when personal information, such as credit card details, has been breached.

See PRIVACY on PAGE A2

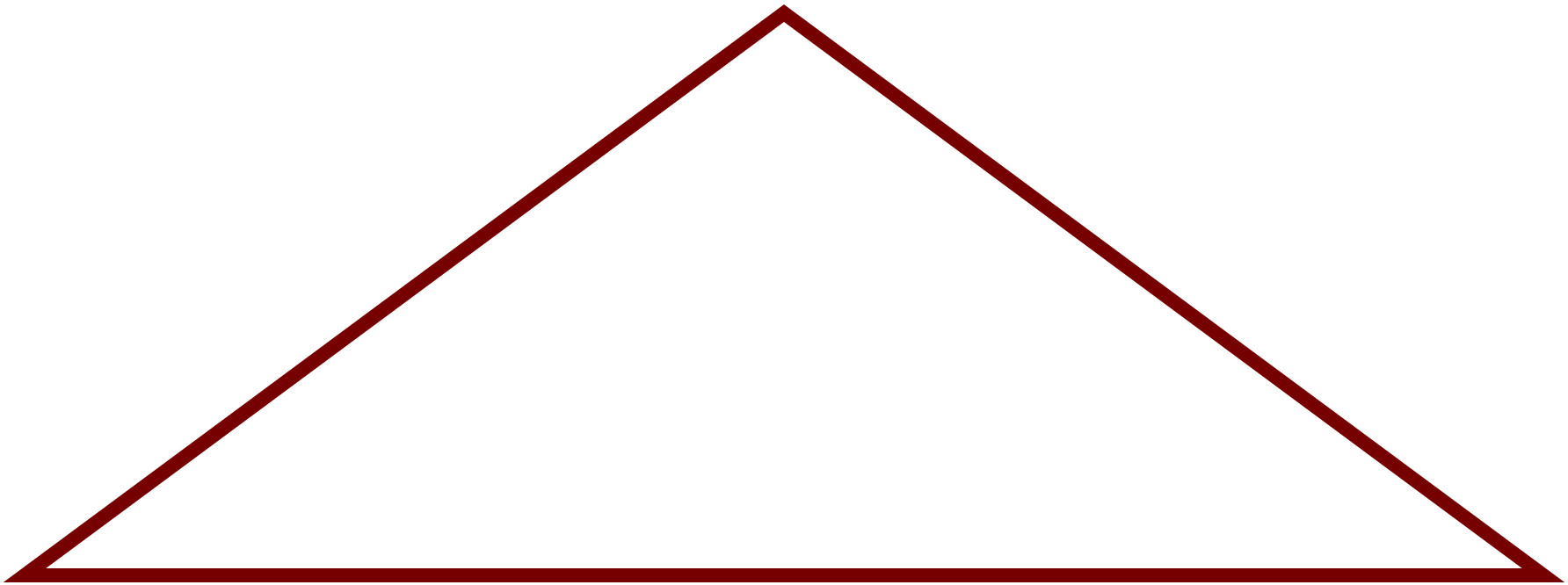
Actual Prediction:
Only One Decade Remains

"Unless we act now, I predict that privacy, as we know it, will be gone – lost, beyond our grasp, by the year 2020."

— Commissioner Cavoukian,
International Conference of Data Protection and Privacy Commissioners,
Jerusalem, October 28, 2010.


PbD
www.privacybydesign.ca

Privacy by Design:
The Trilogy of Applications



Privacy by Design: The 7 Foundational Principles

1. ***Proactive*** not ***Reactive***:
   Preventative not Remedial;
2. Privacy as the ***Default***;
3. Privacy ***Embedded*** into Design;
4. ***Full*** Functionality:
   Positive-Sum, not Zero-Sum;
5. End-to-End **Security**:
   Lifecycle Protection;
6. Visibility ***and*** Transparency;
7. Respect for User Privacy:
   Keep it User Centric.

PbD

www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

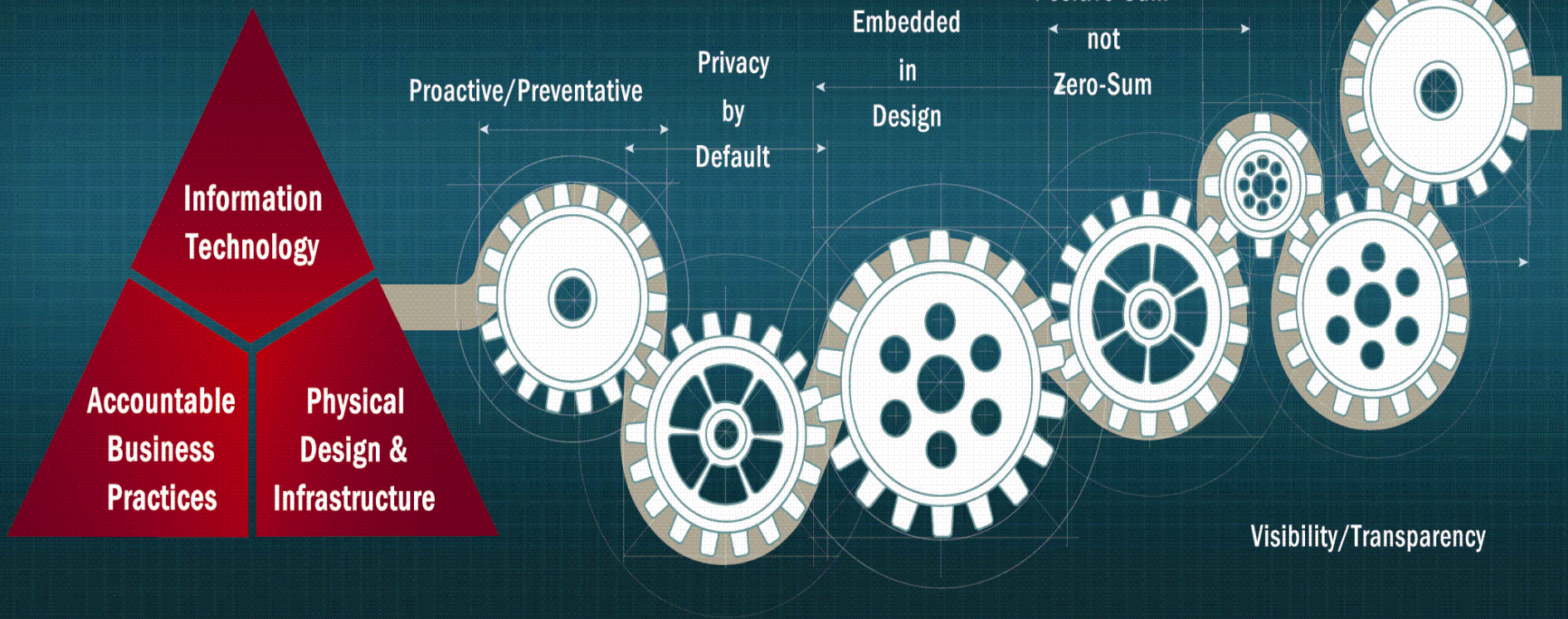
Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

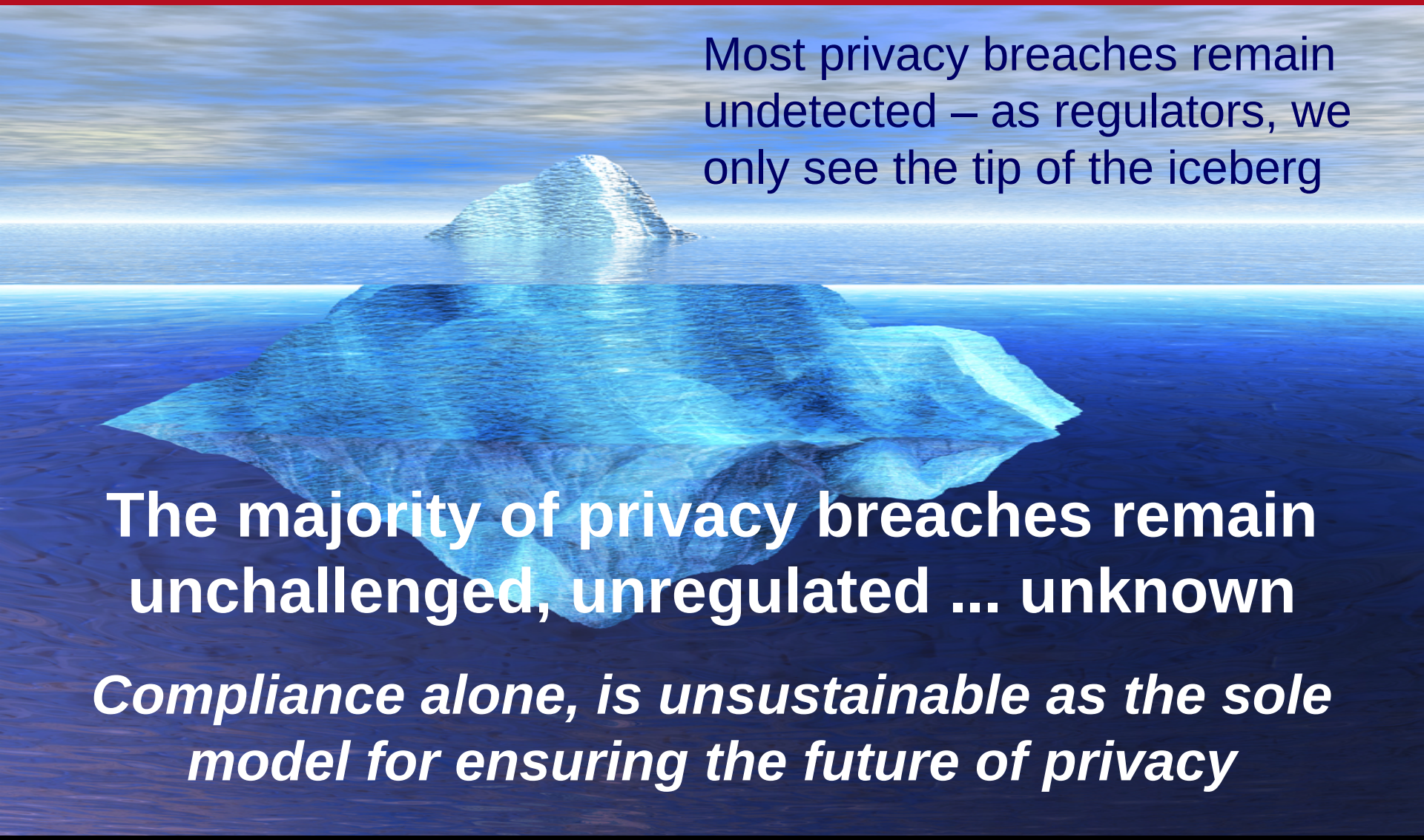
The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Privacy by Design



Why We Need *Privacy by Design*



The majority of privacy breaches remain unchallenged, unregulated ... unknown

Compliance alone, is unsustainable as the sole model for ensuring the future of privacy

Adoption of "Privacy by Design" Resolution

Landmark Resolution Passed to Preserve the Future of Privacy

By Anna Ohlden – October 29th 2010 - http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

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

Full Article:

http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

Adoption of "Privacy by Design" Resolution

- **October, 2010** – regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection:
  - Encourage the adoption of the principles of *PbD* as part of an organization's **default** mode of operation;
  - Invite Data Protection and Privacy Commissioners to promote *PbD*, foster the incorporation if its *7 Foundational Principles* in privacy policy and legislation in their respective jurisdictions, and encourage research into *PbD*.

Embedding Privacy at the Design Stage: *The Obvious Route*

- ***Cost-effective***
- ***Proactive***
- ***User-centric***
- ***It's all about control – preserving personal control over one's data flows***

Personal Health Information Protection Act (PHIPA)

Unique Characteristics of Personal Health Information

- Highly sensitive and personal in nature;
- Must be shared immediately and accurately among a range of health care providers for the benefit of the individual;
- Widely used and disclosed for secondary purposes that are seen to be in the public interest (e.g., research, planning, fraud investigation, quality assurance);
- Dual nature of personal health information is reflected in *PHIPA*, and all other health privacy legislation.

IPC Philosophy – *The 3 C's*

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

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

Why Privacy is Essential to Good Health

- People may engage in privacy protective behaviour if they believe their health data is at risk:
  - Avoiding treatment;
  - Avoiding testing;
  - Out of pocket payment;
  - Multiple doctoring;
  - Lying or withholding information from providers;
  - Asking providers to misrepresent diagnosis.

Personal Health Information Protection Act (*PHIPA*)

- Came into force in Ontario on November 1, 2004;
- Applies to organizations and individuals involved in the delivery of health care services (including the Ministry of Health and Long-Term Care);
- The only health sector privacy legislation in Canada based on consent-implied consent within the ***Circle of Care*****,** otherwise, express consent is required;
- The only health sector privacy legislation that was declared to be substantially similar to Canada's federal private sector privacy legislation, *PIPEDA.*

Praise for *PHIPA*

- In 2009, my office was asked to participate in the U.S. National Institute of Health's (NIH) proposal to build upon the recommendation of the Institute of Medicine's (IOM) Committee on Health Research and Privacy to develop a new approach to protecting privacy in health research (improving on the *HIPAA* Privacy Rule);

- In the IOM report, the only existing statute noted – pointed to as serving a viable framework for revision – was Ontario's *PHIPA.*

Technology-Related Health Orders Under PHIPA

Unencrypted Mobile Devices

- Since *PHIPA* came into force in 2004, I have issued ***nine*** Health Orders;
- ***Four*** of those related to **unencrypted** mobile devices;
- As Commissioner, I find this to be ***completely unacceptable.***

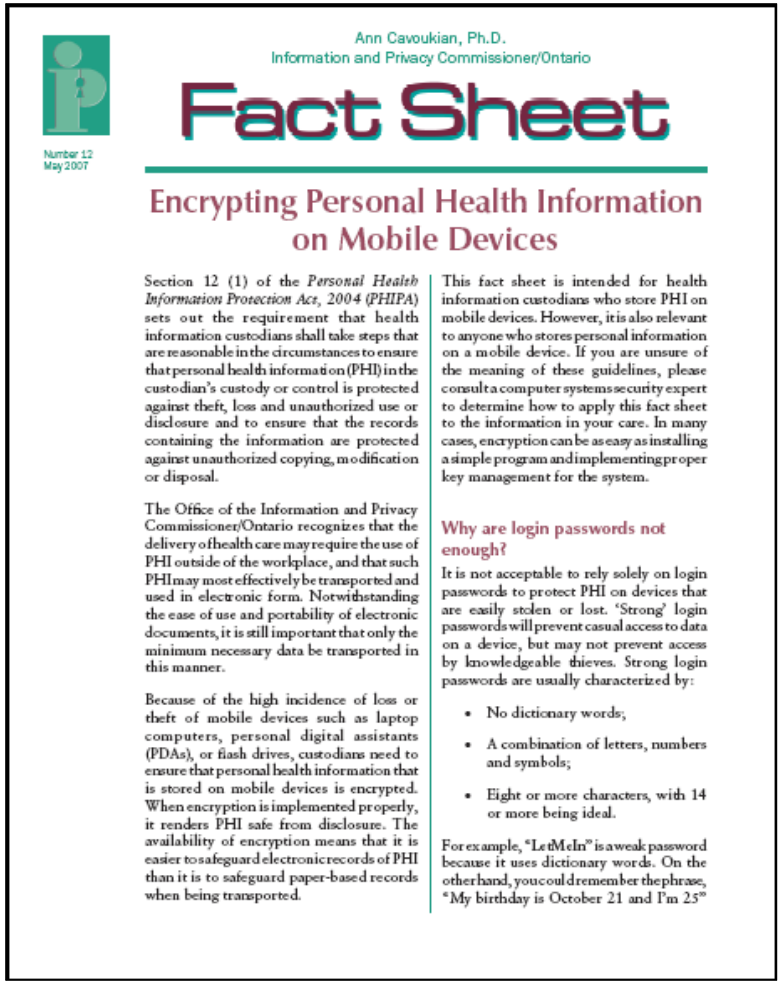
Health Orders Regarding Unencrypted Mobile Devices

- **HO-004** (2007) – Physician at SickKids Hospital had his ***unencrypted laptop*** stolen from his car containing the PHI of 2,900 patients involved in research studies;
- **HO-005 (**2007) – ***Unencrypted Video*** of a patient in the washroom of a methadone clinic appeared on a wireless mobile rear-assist parking device (back-up camera), in a car parked near the clinic;
- **HO-007** (2009) – Nurse lost an ***unencrypted USB key*** containing the PHI of nearly 84,000 people who had attended H1N1 immunization clinics in Durham Region;
- **HO-008** (2010) – Nurse had a ***unencrypted laptop*** stolen from her car containing 20,000 patient records with names, medical records, surgeries performed and physician information.

Fact Sheet #12

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.



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

Fact Sheet

Number 12
May 2007

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.

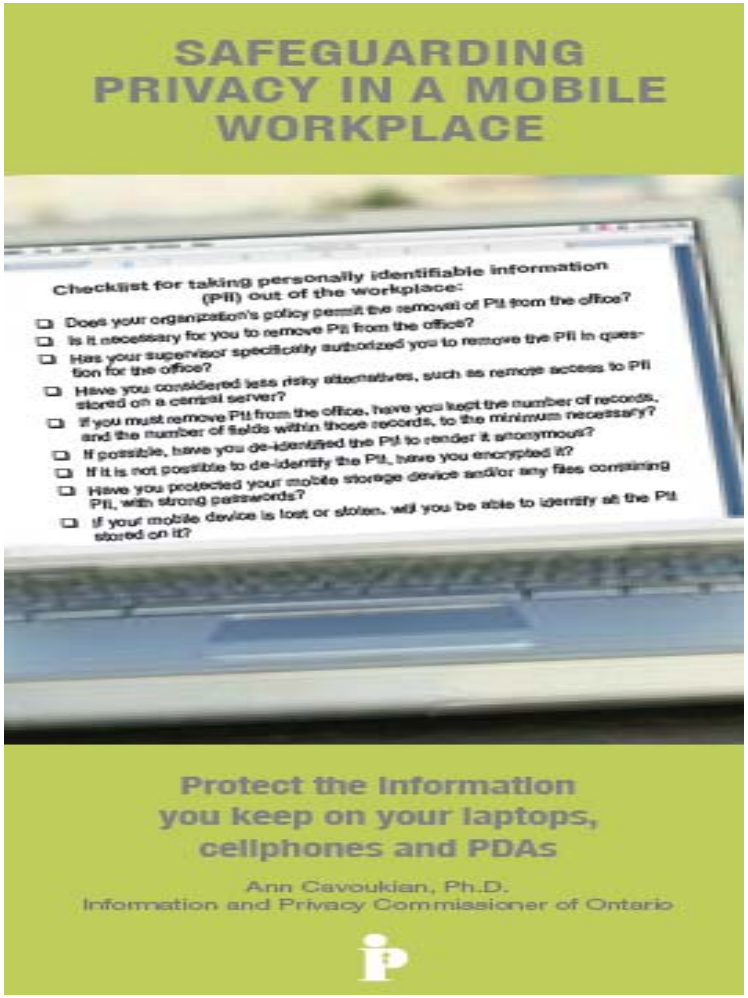
For example, "LetMeIn" is a weak password because it uses dictionary words. On the other hand, you could remember the phrase, "My birthday is October 21 and I'm 25"

www.ipc.on.ca/images/Resources/up-fact_12e.pdf

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 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

Fact Sheet # 16
Health-Care Requirement for Strong Encryption

- Secure Implementation;
- Secure Encryption Keys;
- Secure Authentication of Users;
- No Unintended Creation of Unencrypted Data;
- Identified, Authorized and Trained Users;
- Encryption by Default;
- Availability and Life Cycle Protection;
- Threat and Risk Assessment.

Ann Cavoukian, Ph.D., Information & Privacy Commissioner of Ontario, Canada
Ross Fraser, CISSP, ISSAP, Information Security Consultant

Number 16
July 2010

Fact Sheet

Health-Care Requirement for Strong Encryption

The Office of the Information and Privacy Commissioner (IPC), in Order HO-004, and most recently in Order HO-007, required that health information be safeguarded at all times, specifically by ensuring that any personal health information stored on any mobile devices (e.g., laptops, memory sticks, PDAs) be strongly encrypted.[1] The Order did not otherwise define what constitutes "strong encryption" in the context of protecting the confidentiality, integrity, and availability of personal health information.

Accordingly, this paper provides a working definition of strong encryption and discusses the minimum functional and technical requirements of what may be considered to be strong encryption in a health-care environment. These, in turn, will provide procurement criteria that, if met, will ensure that personal health information stored on encrypted mobile devices or storage media will remain accessible to authorized users, but no one else.

Special thanks go to Dr. Robert Kyle, Durham Region Commissioner and Medical Officer of Health, for supporting the production of this paper.

Strong Encryption

Introduction

The term 'strong encryption' does not refer to a particular technical or design specification, or even to a specific encryption feature that could be inserted into a procurement or audit specification. No particular encryption technology — no matter how 'strong' it may be — can ever, by itself, ensure that information remains secure. Instead, a variety of circumstances and factors need to be taken into account to ensure that personal information is protected against access by unauthorized parties.

To begin with, a good encryption algorithm must be used — one that has been subjected to rigorous peer review. Next, the algorithm must be properly implemented. This may only be confirmed if the encryption system is tested by an independent security testing lab. Once the encryption system is deployed, the encryption keys must be protected and managed effectively. Users who are authorized to decrypt data must be securely authenticated by means of passwords, biometrics, or security tokens. Systems must not leave unencrypted copies of data in web browser caches or on laptop

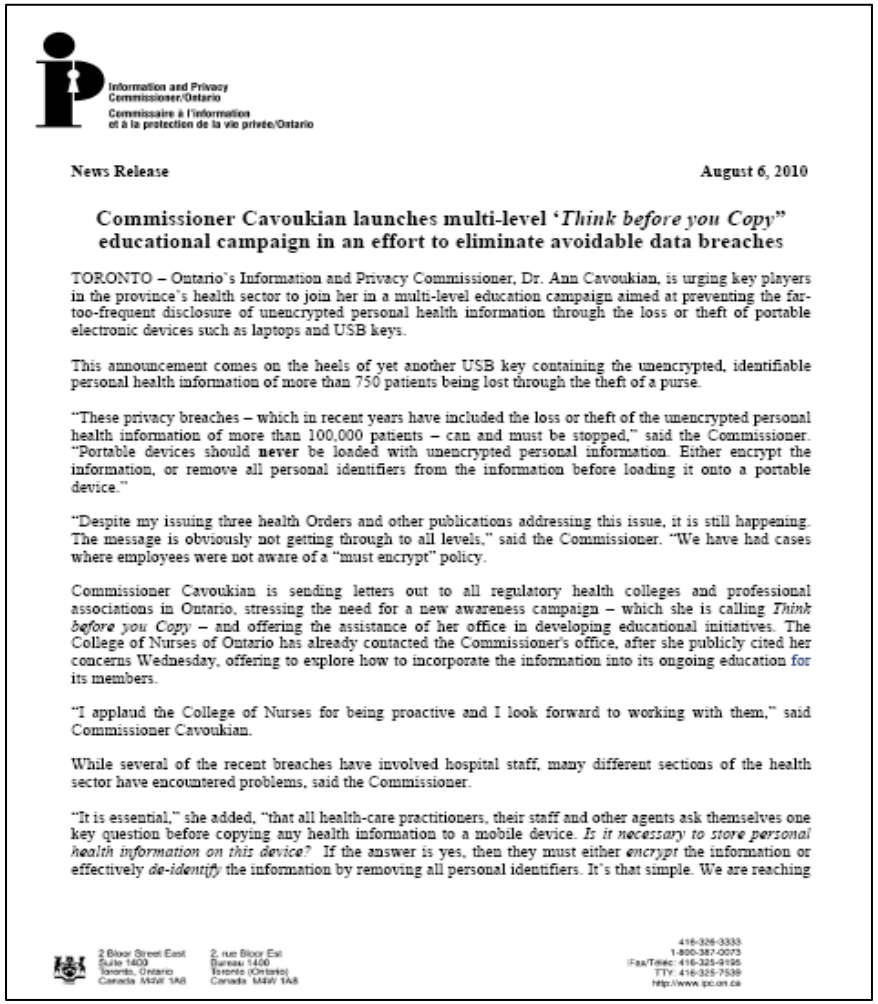
www.ipc.on.ca/images/Resources/fact-16-e.pdf

Stop. Think. Protect

…Protecting Personal Health Information on Mobile and Portable Devices

IPC Campaign: *"Think before you copy"*

- Urging key players in the province's health sector to join in a multi-level education campaign;
- *"Portable devices should never be loaded with unencrypted personal information. Either encrypt the information, or remove all personal identifiers from the information before loading it onto a portable device."*



Information and Privacy Commissioner/Ontario
Commissaire à l'information et à la protection de la vie privée/Ontario

News Release **August 6, 2010**

Commissioner Cavoukian launches multi-level '*Think before you Copy*" educational campaign in an effort to eliminate avoidable data breaches

TORONTO – Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, is urging key players in the province's health sector to join her in a multi-level education campaign aimed at preventing the far-too-frequent disclosure of unencrypted personal health information through the loss or theft of portable electronic devices such as laptops and USB keys.

This announcement comes on the heels of yet another USB key containing the unencrypted, identifiable personal health information of more than 750 patients being lost through the theft of a purse.

"These privacy breaches – which in recent years have included the loss or theft of the unencrypted personal health information of more than 100,000 patients – can and must be stopped," said the Commissioner. "Portable devices should **never** be loaded with unencrypted personal information. Either encrypt the information, or remove all personal identifiers from the information before loading it onto a portable device."

"Despite my issuing three health Orders and other publications addressing this issue, it is still happening. The message is obviously not getting through to all levels," said the Commissioner. "We have had cases where employees were not aware of a "must encrypt" policy.

Commissioner Cavoukian is sending letters out to all regulatory health colleges and professional associations in Ontario, stressing the need for a new awareness campaign – which she is calling *Think before you Copy* – and offering the assistance of her office in developing educational initiatives. The College of Nurses of Ontario has already contacted the Commissioner's office, after she publicly cited her concerns Wednesday, offering to explore how to incorporate the information into its ongoing education for its members.

"I applaud the College of Nurses for being proactive and I look forward to working with them," said Commissioner Cavoukian.

While several of the recent breaches have involved hospital staff, many different sections of the health sector have encountered problems, said the Commissioner.

"It is essential," she added, "that all health-care practitioners, their staff and other agents ask themselves one key question before copying any health information to a mobile device. *Is it necessary to store personal health information on this device?* If the answer is yes, then they must either *encrypt* the information or effectively *de-identify* the information by removing all personal identifiers. It's that simple. We are reaching

2 Bloor Street East Suite 1400 Toronto, Ontario Canada M4W 1A8
2, rue Bloor Est Bureau 1400 Toronto (Ontario) Canada M4W 1A8
416-326-3333 1-800-387-0073 Fax/Téléc: 416-325-9195 TTY: 416-325-7539 http://www.ipc.on.ca

www.ipc.on.ca/images/Resources/2010-08-06-think-nr.pdf

STOP

Ask yourself:

Do I really need to store any personal health information on this device?

THINK

- Consider the alternatives;
- Would de-identified or encoded information serve the same purpose?

- Can you access the information remotely through a secure connection or virtual private network (VPN) instead?

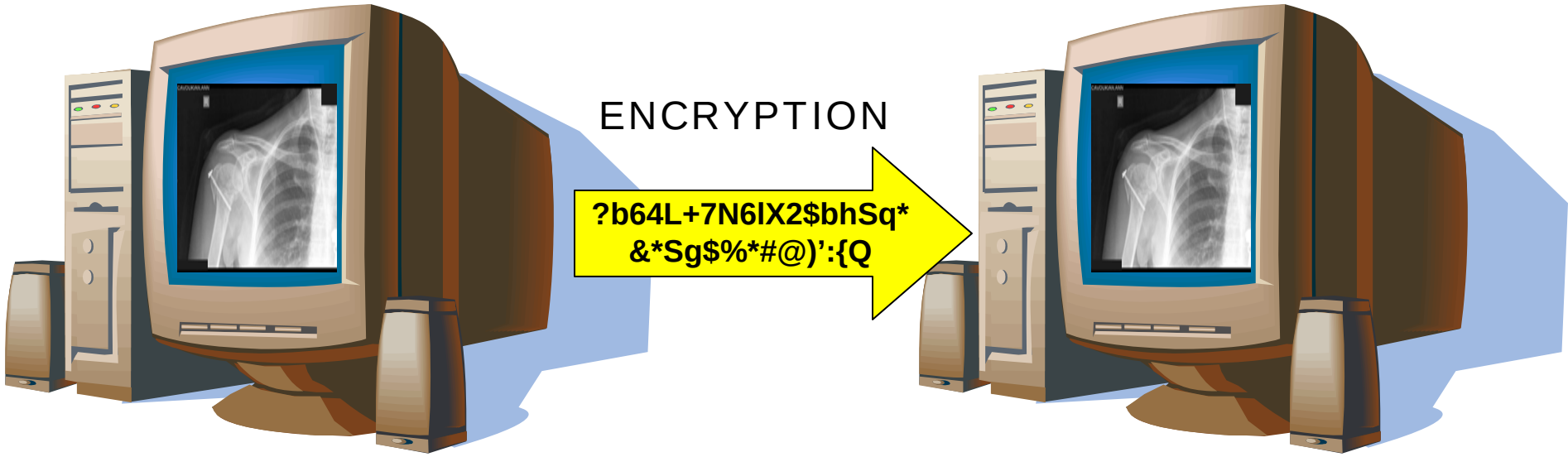
PROTECT

If you **must** store personal health information on a mobile device:

- Make sure it is strongly encrypted and protected with passwords;
- Store the least amount of information for the shortest amount of time;
- Develop policy and procedures for the secure retention on mobile or portable devices – including training for agents and audit compliance on the policies and procedures.

What is Encryption?

- It means encoding information to render it meaningless through an array of letters, numbers and symbols;
- It is accomplished through the use of a computer algorithm and encryption keys.



What is Strong Encryption?

- Does not refer to a particular technical or design specification or a specific encryption feature;
- Refers to the high degree of confidence that plaintext personal health information will not be disclosed to unauthorized persons;
- Strong encryption includes ensuring that:
  - An up-to-date encryption algorithm that is consistent with industry standards and practices is used;
  - Encryption is thoroughly integrated into operations and is supported by security policies, procedures and practices;
  - Encryption is operational, by default.

What is Strong Encryption? (Cont'd)

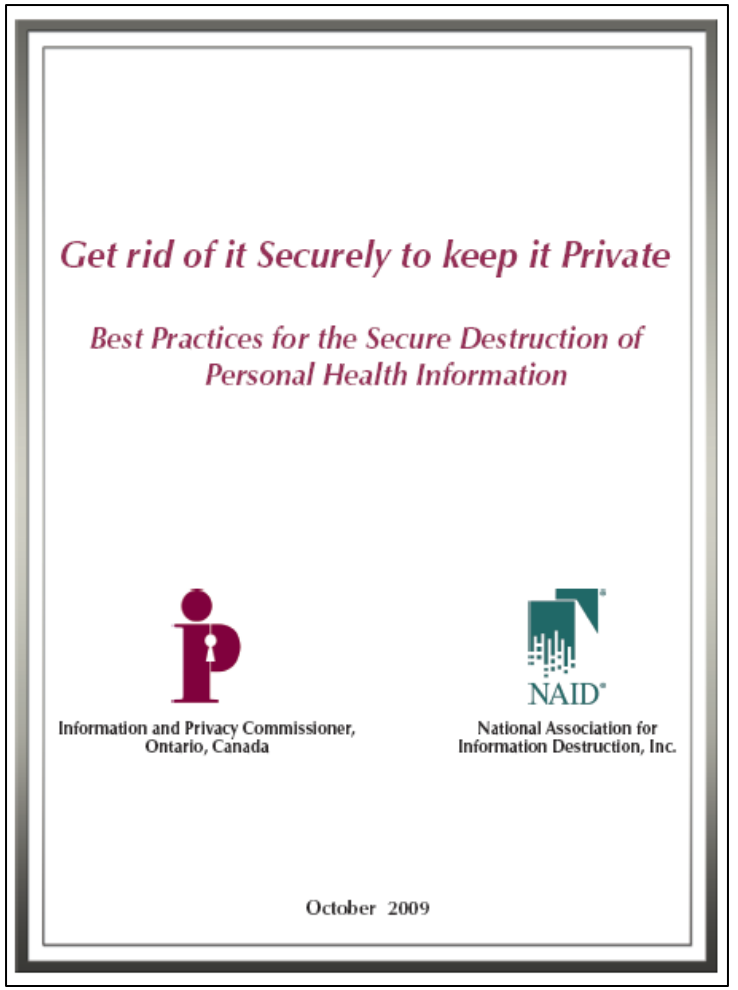
- Strong encryption also includes ensuring that:
  - The encryption solution has been successfully deployed;
  - The encryption solution continues to function appropriately;
  - Error messages indicating a malfunction of the encryption solution are monitored and responded to immediately;
  - Encryption keys of a sufficient length are used;
  - Safeguards are implemented to protect encryption keys from theft, loss and access by unauthorized persons;
  - The encryption solution is subject to ongoing security reviews and updates.

What Are Strong Passwords?
What Is Strong Password Protection?

- Strong passwords consist of at least eight characters;
- Strong passwords combine letters, numbers and symbols in what appear to be random string;
- Strong password protection includes the development and implementation of policies and procedures:
  - Identifying the minimum and maximum password length;
  - Outlining the standard for password composition;
  - Providing for automatic expiry after a defined period;
  - Requiring that the device be locked after a defined number of failed log-in attempts;
  - Imposing a mandatory system-wide password-protected screen saver after a pre-defined period of inactivity;
  - Requiring agents to keep passwords private (i.e. not writing down or sharing passwords).

Get Rid of it Securely to Keep it Private –
Best Practices for the Secure Destruction of Personal Health Information

1. Develop and implement a secure destruction policy;
2. Segregate and securely store personal health information;
3. Determine best methods of destruction;
4. Document the destruction process;
5. Considerations prior to employing a service provider;
6. Disposal of securely destroyed materials;
7. Auditing and ensuring compliance.



www.ipc.on.ca/images/Resources/naid.pdf

Conclusions

- Lead with ***Privacy by Design*** – embed privacy into the design specifications of IT, accountable business practices and networked infrastructure;
- In the process, change the paradigm from zero-sum to positive-sum, whereby both privacy and any other functionality may be delivered, thereby raising the overall level of protection;
- When you change the paradigm, you change the mindset: you can deliver both privacy AND functionality, not as a mutually exclusive "either/or" (a false dichotomy), but as the doubly-enabling "win/win;"
- Through planning, education and training, new health privacy laws should not pose an obstacle to the delivery of effective health care.

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