Minimize Risk – Maximize Protection, Gain A Competitive Advantage: *Privacy is Good for Business*

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Risk & Insurance Management Society
RIMS Canada 2008 Conference
September 24, 2008

Presentation Outline

1. *Privacy "101" – Setting the Stage*
2. *Identity Theft, Phishing and Pharming*
3. *Privacy Legislation: PIPEDA & PHIPA*
4. *Why Privacy is Good for Business*
5. *Consumer Confidence and Trust*
6. *Managing Your Data: Do You Have A Map?*
7. *Transformative Technologies*

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 ≠ Security

Privacy and Security:
The Difference

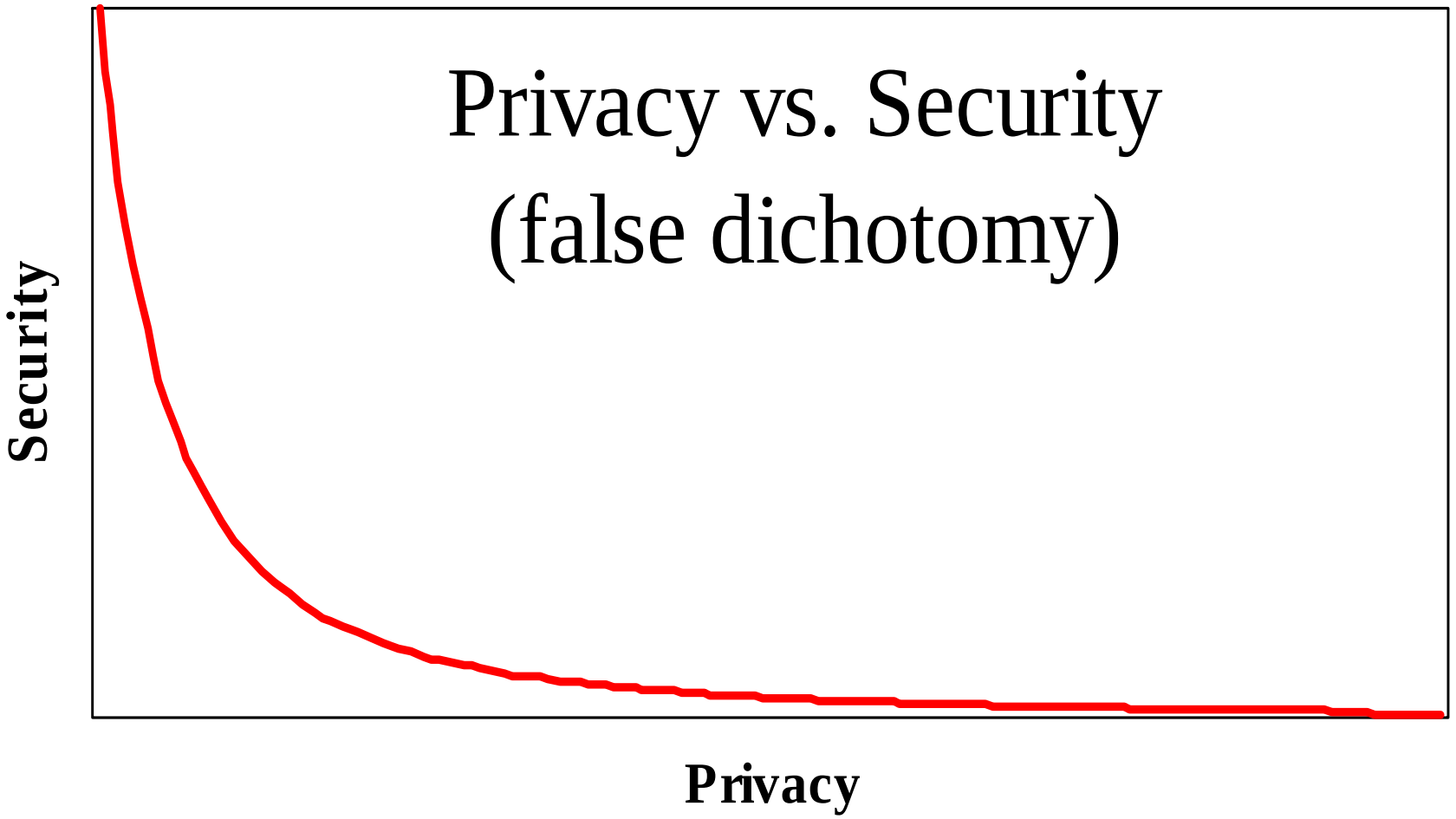
- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation

Security:

Organizational control of information through information systems

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

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,
not an "either/or"
involving trade-offs

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).

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

Canada's Fair Information Practices

- **Accountability**
- **Identifying Purposes**
- **Consent**
- **Limiting Collection**
- **Limiting Use, Disclosure, Retention**
- **Accuracy**
- **Safeguards**
- **Openness**
- **Individual Access**
- **Challenging Compliance**

Personal Information Protection and Electronic Documents Act, 2000
www.privcom.gc.ca/legislation/02_06_01_01_e.asp

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 disclosures;
- **Who will be able to see my information?**
  - Restricted access from unauthorized third parties.

Identity Theft, Phishing and Pharming

Identity Theft

- The fastest growing form of consumer fraud in North America;
- Identity theft is the most frequently cited complaint received by the F.T.C. – almost half of total complaints received;
- During 2007, the FTC received 813,899 consumer fraud and identity theft complaints; up 21% over 2006;

— Federal Trade Commission, 2008

- The Canadian Anti-fraud Call Centre (CAFCC) reported some 10,000 complaints of identity theft and identity fraud with losses totalling more than $6 million in 2007 – and more than $1 million in the first quarter of 2008;
- The CAFCC estimates the numbers actually represent a very small percentage of the actual figures due to unreported cases.

— Criminal Intelligence Service Canada, 2008

Cost of Identity Theft in Canada

Theft and fraud are costing Canadian businesses **$8 million a day**, or more than **$3 billion a year;**

According to the Retail Council of Canada:

- Credit card fraud in Canada resulted in losses of **$201 million** to major credit card companies in 2005;
- Debit card fraud resulted in losses of **$70.4 million**.

— Mario Toneguzzi, *Theft, fraud cost retailers $8 million a day*, Ottawa Citizen, March 2, 2007.

Phishing and Pharming

- Fraudulent online capture and misuse use of personal information;
- Significant economic consequences – a root cause of identity theft and other deceptive practices;
- How can individuals be certain of the identity of companies online – ***are they real?***
- Companies' reputations and brands are impacted by deceptive online practices.

Phishing and Pharming (Cont'd)

- Phishing is like spam but more sophisticated – it's targeted and malicious;
- A criminal activity, phishing is perceived as an invasion of privacy;
- Phishing may involve installing spyware on individuals' computers;
- The phishing problem is skyrocketing and, ***no one is immune;***
- Pharming is technological exploitation that tricks users into visiting a fraudulent website.

Privacy Legislation: PIPEDA & PHIPA

Federal Privacy Law: *PIPEDA*

- The *Personal Information Protection and Electronic Documents Act* governs how private-sector organizations collect, use and disclose personal information in the course of commercial business. In addition, the *Act* contains various provisions to facilitate the use of electronic documents;

- It was passed in the late 1990s to promote consumer trust in electronic commerce and also to reassure the European Union that Canadian privacy laws were adequate to protect the personal information of European citizens;

- *PIPEDA* incorporates and makes mandatory provisions of the Canadian Standards Association's Model Code for the Protection of Personal Information.

PIPEDA – www.privcom.gc.ca/legislation/02_06_01_01_e.asp
CMA Model Code – www.csa.ca/standards/privacy/Default.asp?language=english

Extension of *PIPEDA*

- As of January 1, 2004, *PIPEDA* has extended to:
- All personal information collected, used or disclosed in the course of commercial activities by provincially regulated organizations (including insurance companies and independent insurance adjusters);
- *PHIPA* is the only health sector privacy legislation to be declared to be substantially similar to Canada's federal private sector law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

PIPEDA
General Consent Rule

- Assume that both insurance company and adjuster are in Ontario (*PIPEDA would* apply);
- Knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate;
- In insurance claims where there is no suspicion of fraud, adjuster should only collect, use and disclose personal information with the knowledge and consent of the policyholder.

Fraud Investigations

- *PIPEDA* recognizes a public interest in collecting, using and disclosing personal information without the knowledge and consent of the individuals for the purpose of fraud investigations;
- Privacy is not an absolute right – occasionally, it needs to be balanced against other interests.

Consent Exceptions in *PIPEDA*

- "Investigative bodies" designated in regulations may receive and disclose personal information without the knowledge and consent of the individual, to investigate a breach of an agreement or a contravention of the laws of Canada or a province.

PIPEDA Regulations

- November 6, 2003 – Industry Canada issued notice to amend *PIPEDA* regulations to include additional organizations as “investigative bodies;”
- Insurance adjusters and private investigators were included (among others).

Protecting Privacy During Investigations

- "Investigative body" status will not give insurance adjusters unlimited power to collect, use and disclose personal information without consent;
- Adjusters should only collect, use and disclose minimum amount of personal information necessary for purposes of investigation;
- They should also ensure that any third parties that are retained (e.g., private investigators) do not violate privacy laws when assisting with claims investigations.

Provincial Health Privacy Laws

- Alberta
  - *Health Information Act* (HIA)
- Manitoba
  - *Personal Health Information Act* (PHIA)
- **Ontario**
  - ***Personal Health Information Protection Act* (PHIPA)**
- Saskatchewan
  - *Health Information Protection Act* (HIPA)

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.

Privacy in the Context of Health Care

- Privacy is not a new issue in the health care context – all medical staff are well aware of the privacy issues;
- *PHIPA* was drafted in a manner such that privacy would not impede the delivery of health care services;
- Health information custodians may imply consent for the collection, use and disclosure of personal health information for the delivery of health care services;
- Express consent is required when personal health information is disclosed to a person who is not a health information custodian, or for a purpose other than the delivery of health care services.

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**.

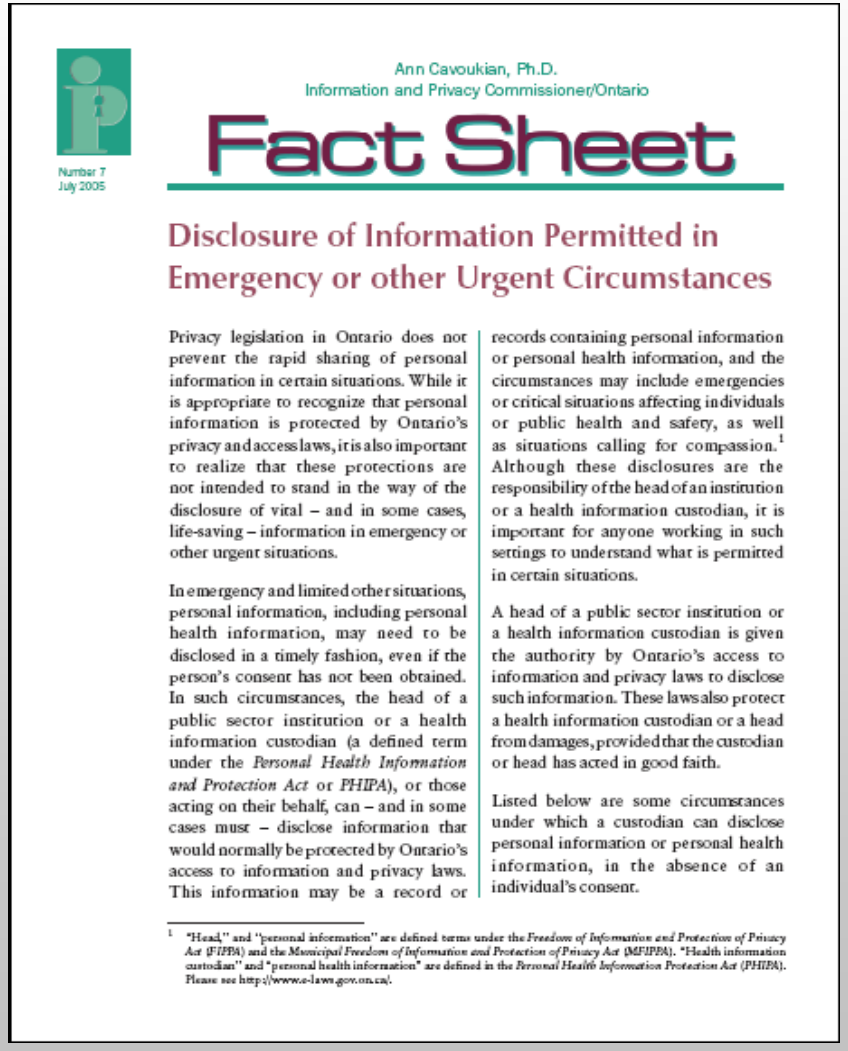
Permissible Disclosures:
Safety and Law Enforcement Purposes

Derogations from the consent principle are allowed in limited circumstances, for example:

- To protect the health or safety of the individual or others (s. 40(1)).
- To a person carrying out an inspection, investigation or similar procedure that is authorized by a warrant or by law (s. 43(1)(g)).
- As required by law (s. 43(1)(h)).

Disclosure of Information Permitted in Emergency or other Urgent Circumstances

- Public Interest and Grave Hazards
- Health and Safety of an Individual/ Risk of Serious Harm to Person or Group
- Disclosures to Public Health Authorities
- Compassionate Circumstances
- Providing Health Care
- Liability protection



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

Number 7
July 2005

Fact Sheet

Disclosure of Information Permitted in Emergency or other Urgent Circumstances

Privacy legislation in Ontario does not prevent the rapid sharing of personal information in certain situations. While it is appropriate to recognize that personal information is protected by Ontario's privacy and access laws, it is also important to realize that these protections are not intended to stand in the way of the disclosure of vital – and in some cases, life-saving – information in emergency or other urgent situations.

In emergency and limited other situations, personal information, including personal health information, may need to be disclosed in a timely fashion, even if the person's consent has not been obtained. In such circumstances, the head of a public sector institution or a health information custodian (a defined term under the *Personal Health Information and Protection Act* or *PHIPA*), or those acting on their behalf, can – and in some cases must – disclose information that would normally be protected by Ontario's access to information and privacy laws. This information may be a record or records containing personal information or personal health information, and the circumstances may include emergencies or critical situations affecting individuals or public health and safety, as well as situations calling for compassion.[1] Although these disclosures are the responsibility of the head of an institution or a health information custodian, it is important for anyone working in such settings to understand what is permitted in certain situations.

A head of a public sector institution or a health information custodian is given the authority by Ontario's access to information and privacy laws to disclose such information. These laws also protect a health information custodian or a head from damages, provided that the custodian or head has acted in good faith.

Listed below are some circumstances under which a custodian can disclose personal information or personal health information, in the absence of an individual's consent.

[1] "Head," and "personal information" are defined terms under the *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*. "Health information custodian" and "personal health information" are defined in the *Personal Health Information Protection Act (PHIPA)*. Please see http://www.e-laws.gov.on.ca/.

www.ipc.on.ca/images/Resources/up-3fact_07_e.pdf

Investigations – Section 43(1)(g)

- Section 43(1)(g) of *PHIPA* allows a health information custodian to disclose personal health information about an individual " … to a person carrying out an inspection, investigation or similar procedure that is authorized by a warrant or by or under this *Act* or any other *Act* of Ontario or Canada for the purpose of complying with the warrant or for the purpose of facilitating the inspection, investigation or similar procedure."

Why Privacy is Good for Business

The Bottom Line

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

Think of privacy as a sound business strategy

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.

Consumer Confidence and Trust

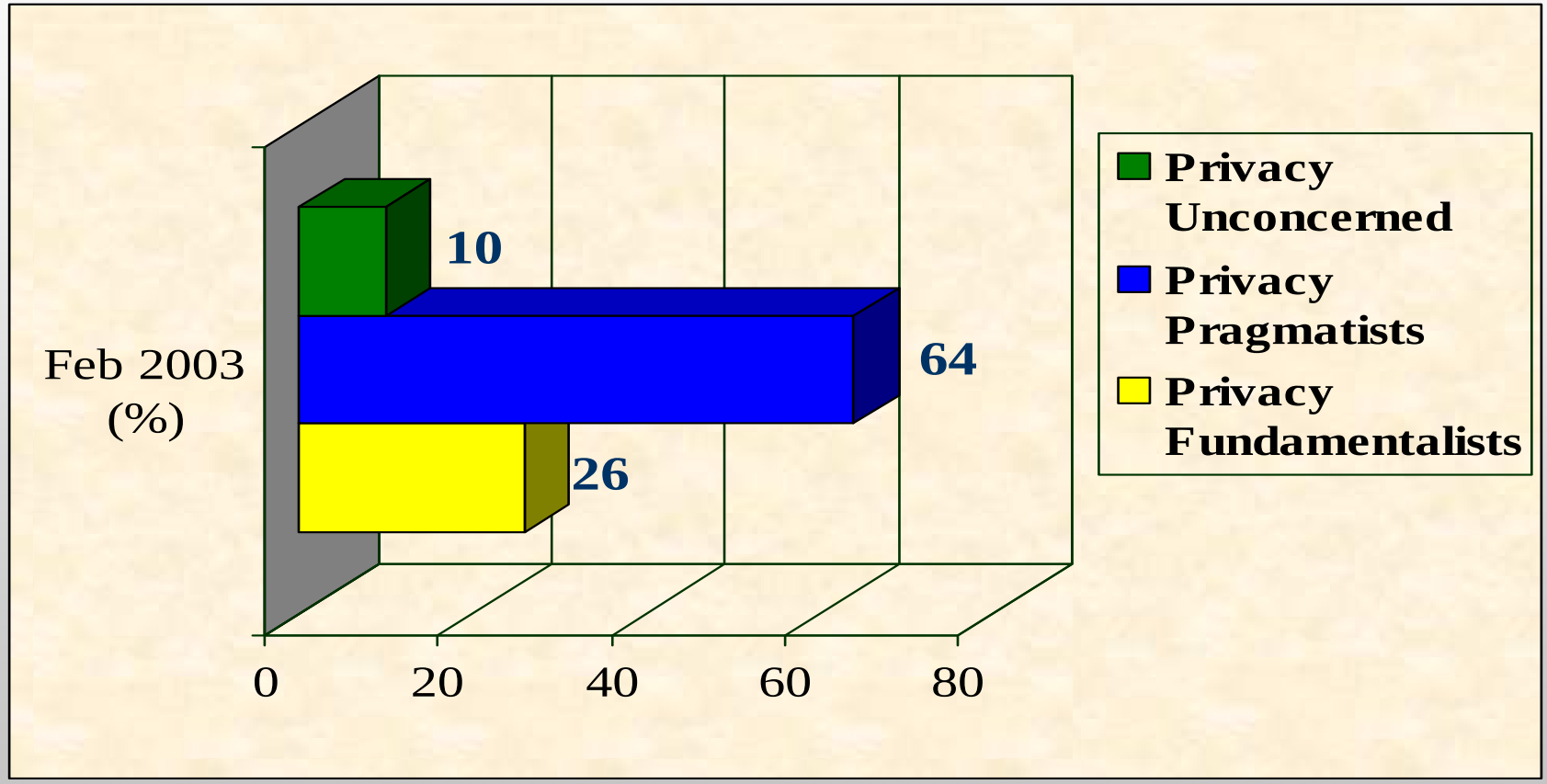
Consumer Trust is the Key

A simple fact about online behaviour:

- Increased trust online breeds more online customers;
- The key to increasing online commerce is to draw in new consumers by removing the barriers to consumer trust.

— Isaac Scarborough, *Consumers Still Don't Trust the Internet*, imediaconnection.com, November 14, 2005.

How The Public Divides on Privacy



— Dr. Alan Westin,
The "Privacy Dynamic" – Battle for the minds of the pragmatist, 2001.

Managing Your Data: Do You Have A Map?

Managing Your Data

- Does your organization have a Data Map?
- Do you know all the points of entry for personally identifiable information (PII) into your organization?
- Do you know how customer data flows throughout your organization?
- Do you have a consent management system in place … when you need to obtain additional consent from your customers?

Privacy and Security Risks in Telecommuting

Ernst & Young 2008 Survey on Telecommuting:

- Only **50%** of companies surveyed had guidelines for telecommuting in place;
- **50%** of employees use personal devices from time to time, but security required for corporate devices is seldom applied;
- Nearly **75%** of companies allow telecommuters to generate paper records containing personal information;
- **30%** of companies require shredding of records, but do not supply shredders; and **25%** require secure storage, but do not provide cabinets;
- **17%** have no secure disposal (shredding) requirements;
- **20%** periodically audit telecommuters' physical environments.

www.cdt.org/privacy/20080729_riskathome.pdf

Assess Your Risks

Assess your risks to privacy:

- Conduct a privacy impact assessment;
- Follow up with independent privacy audits using Generally Accepted Privacy Principles (GAPP) **http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+ Principles/**

Transformative Technologies

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

Positive-Sum Paradigm

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

Transformative Technologies

Surveillance Technology + Positive-Sum Paradigm + Privacy Enhancing Technology =

<u>Transformative Technologies</u>

Common characteristics of Transformative Technologies:

- Help minimize unnecessary disclosure, collection, retention and use of personal data;
- Empower individuals to participate in the management of their personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in (personal) data governance structures;
- Help promote and facilitate widespread adoption of those technologies.

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