The Privacy Imperative:
Go Beyond Compliance to Competitive Advantage

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner of Ontario

Arizona State University

School of Management

April 11, 2006

What is Privacy?

Impetus for Change

- Growth of Privacy as a Global Issue

  (EU Directive on Data Protection);

- Exponential growth of personal data collected, transmitted and exploited;

- Convergence of growth in bandwidth, sensors, data storage and computing power;

- Consumer Backlash; heightened consumer expectations.

And then came 9/11

- U.S. Patriot Act and series of anti-terrorism laws introduced;
- Served to expand powers of surveillance on the part of the state, and reduce judicial oversight;
- Polarized debate for **Security versus Privacy**.

Change the Paradigm

- Old Paradigm: Zero Sum Game;
- New Inclusive Paradigm: STEPs:
  (Security Technologies Enabling Privacy);
- Expand the discourse: *Privacy* and *Security* are not polar opposites — both are essential.

http://www.ipc.on.ca/docs/steps.pdf

The Aftermath

It’s business as usual:

– Clear distinction between public safety and business issues – make no mistake: business expectations remain high;

– NO reduction in consumer expectations;

– Increased value of trusted relationships.

Consumer Attitudes

- **Business is not a beneficiary of the post-9/11 "Trust Mood"**
- Increased trust in government has not been paralleled by increased trust in business handling of personal information.

— *Privacy On and Off the Internet: What Consumers Want*

Harris Interactive, November 2001

Dr. Alan Westin

Importance of Consumer Trust

In the post-9/11 world:

- Consumers either as concerned or **more** concerned about online privacy;
- Concerns focused on the **business** use of personal information, not new government surveillance powers.

Consumer attitudes and actions toward businesses with regards to privacy:

- **83%** refused to give personal information;
- **81%** requested not to give or sell their personal information to another company;
- **67%** would not register at a website because they were unsure how their data would be used;
- **60%** declined to do business with a company because they were unsure how their personal information would be used.

— Dr. Alan Westin, *Consumer Privacy: Attitudes and Actions*, January 2005.

Information Privacy Defined

- **Information Privacy: Data Protection:**
  - Freedom of choice; control; informational self-determination;
  - Personal control over the collection, use and disclosure of any recorded information about an identifiable individual.

What Privacy is Not

Security ≠ Privacy

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

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Eight Principles:

1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

United States
Safe Harbor, 2000

Safe Harbor Privacy Principles:

1. Notice
2. Choice
3. Onward Transfer
4. Security
5. Data Integrity
6. Access
7. Enforcement

As of April 1, 2006, there were 913 businesses signed under the Safe Harbor Agreement.

Safe Harbor Principles Requirements

Organizations signed under safe harbor must comply with seven principles:

1. **Notice:** Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure;
2. **Choice:** Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual;
3. **Onward Transfer** (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent(1), it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles;

Safe Harbor Principles Requirements (Cont'd)

4. **Access:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated;
5. **Security:** Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction;
6. **Data integrity:** Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current;
7. **Enforcement:** In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

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 Ten Commandments

1. **Accountability:**
    - for personal information designate an individual(s) accountable for compliance;
2. **Identifying Purposes:**
    - purpose of collection must be clear at or before time of collection;
3. **Consent:**
    - individual has to give consent to collection, use, disclosure of personal information;

The Ten Commandments

4. **Limiting Collection:**
    - collect only information required for the identified purpose; information shall be collected by fair and lawful means;
5. **Limiting Use, Disclosure, Retention:**
    - consent of individual required for all other purposes;
6. **Accuracy:**
    - keep information as accurate and up-to-date as necessary for identified purpose;
7. **Safeguards:**
    - protection and security required, appropriate to the sensitivity of the information;

The Ten Commandments

8. **Openness:**
   - policies and other information about the management of personal information should be readily available;
9. **Individual Access:**
   - upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and be given access to that information, be able to challenge its accuracy and completeness and have it amended as appropriate;
10. **Challenging Compliance:**
   - ability to challenge all practices in accord with the above principles to the accountable body in the organization.

Problems

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 – *40% of total complaints received*;
- 10 million victims of ID theft each year, costing businesses $50 billion, and $5 billion in out-of-pocket expenses from individuals;

— Federal Trade Commission, 2003

A Sample of Major Privacy Breaches*

Nov 2004: *ChoicePoint* — Identity theft involving 145,000 persons;
Dec 2004: *Bank of America* — 1.2 million records misplaced;
Apr 2005: *TimeWarner* — Lost files on 600,000 employees;
Jun 2005: *Citibank* — Lost files on almost 4 million customers;
Jun 2005: *CardSystems* — Hacker theft of 40 million Visa/MasterCard records;
Jan 2006: *People's Bank* — Lost tapes containing 90,000 customer files;
Feb 2006: *FedEx* — Accidentally exposed 8,500 employee tax forms;
Feb 2006: *OfficeMax* — Hacker accessed 200,000 debit card accounts;
Feb 2006: *Ernst & Young* — Laptop stolen containing 38,000 customer files;
Mar 2006: *Fidelity Investments* — Laptop stolen with 196,000 customer files;
Mar 2006: *Georgia Technology Authority* — Hacker theft of 553,000 pension files.

*****_For a full chronology of data breaches visit Privacy Rights Clearing House at,_
www.privacyrights.org/ar/ChronDataBreaches.htm

Identity Theft: Easier Than You Think

- The popular myth of identity theft is that it is committed by renegade computer geniuses using high-tech methods;
- In fact, these crimes continue to depend on a steady and easily accessible supply of personally identifiable information (PII);
- Nearly 90% of the U.S. population can be uniquely identified through the use of only three pieces of information: a person's date-of-birth, sex, and postal code.

— L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," *Int'l J. Uncertainty, Fuzziness, and Knowledge-Based Systems*, vol. 10, 2002.

Do You Know Where Your Mail Is?

- **March 8, 2006:** ***Canada Post tip leads to arrests in identity scam***

  — Globe and Mail

- Acting on information provided by Canada Post corporate security, Ottawa police uncovered a major crime operation involving identity theft and mail fraud;

- Two persons rented a post office box and took out ads asking anyone wanting to make $70,000 a year to submit their résumé;

- Victims were then mailed a letter declaring that they were suitable candidates and to complete an application form providing their date of birth, driver's licence number, social insurance number, home address and a $20 processing fee;

- That information was then used to obtain credit cards from banks and department stores in addition to driver's licences and social insurance cards in the victim's names.

The Current Privacy Storm

- To date, **twenty-four states** have signed laws that now require consumers to be notified if personal information has been subject to a security breach – a further **nineteen** have proposals for such laws;
- Although the new laws are similar to California's SB1386, ***varying state requirements will likely put pressure on Congress to pass a federal version of SB1386;***
- Legislation is also being considered that would ban the sale of Social Security numbers without the permission of the owner, except when needed by law enforcement;
- June 2005, FTC *"Disposal Rule"*

Data-Breach Notification

States Differ on When to Sound the Alarm

- **January 2006**, the Federal Deposit Insurance Corp discovered that stolen personal information from employees was used to set up fraudulent credit union loans;
- Instead of immediately notifying the affected persons, it kept quiet about the breach for a few months at the request of law enforcement;
- The FDIC's experience mirrors that of many banks trying to navigate a mix of security standards spread between federal regulatory guidelines and a host of new state data security laws;
- Further, a number of state laws also conflict with each other, define breaches differently and prescribe different thresholds for notification triggers, for example:
  - **Illinois** does not allow a notification delay for law-enforcement purposes;
  - **Nevada** and **Minnesota** call for alerts whenever an unauthorized breach occurs;
  - **New Jersey** and **North Carolina** do not exempt encrypted data that would be unusable to most identity thieves.

Data-Breach Notification

Financial Data Protection Act, 2005

- **March 16, 2006:** the House Financial Services Committee passed the ***Financial Data Protection Act, 2005***, which sets out requirements for companies to investigate breaches and notify law enforcement and consumers;
- The law seeks to ease compliance for the financial industry by setting a national standard for data security that overrides state laws;
- However, there is much criticism of the new *Act* as being an *after the fact* protection measure because it requires investigations and notification when the unauthorized use of data was ***likely*** to result in harm or inconvenience to consumers;
- The data security legislation is expected to supersede Gramm-Leach-Bliley which could bring a new set of regulatory requirements on the financial industry.

Comprehensive Security and Technology

- In many instances, physical access to the data or media is all that is needed for a privacy breach to take place;
- Many security breaches can be avoided if simple physical safeguards had been in place and adhered to;
- However, while physical security measures are important, ***they must*** increasingly be supported in depth by organizational and ***technological reinforcements.***

Don’t Blame the Victim

- Violations of privacy can be viewed as an external cost – a negative externality;
- ***Businesses however, not consumers, create privacy externalities through their misuse or lack of sufficient protection of their customers’ personal information;***
- It would be far more costly for individuals to prevent, or attempt to remedy, the abuses of their personal information – if possible at all;
- ***The IPC places the responsibility for protecting customer’s PII squarely upon businesses;***
- IPC Paper: ***Identity Theft Revisited: Security is Not Enough***, www.ipc.on.ca/userfiles/page_attachments/idtheft-revisit.pdf

Poor Information Management Practices at Fault

- Businesses that collect personal information from customers and retain it in their databases must separate the personal identifiers from the transactional data;
- The Gartner Group has estimated that internal employees commit 70% of information intrusions, and more than 95% of intrusions that result in significant financial losses;
- Personal identifiers cannot be left in plain view in databases when linked to transactional data contained in databases;
- Personal identifiers may be separated from transactional data in a variety of ways including encryption, severing, masking, etc.

Technological Reinforcements

Database Encryption:

- After limiting physical access, the single most important action is to secure data by encrypting it, not just in transit, but also in its place of storage.

Severing or Encrypting Personal Identifiers:

- Encrypt or replace certain sensitive database fields, or otherwise sever the personal identifiers from the data record itself.

Data Aggregation, Perturbation and Anonymization:

- Effectively strip away key identifiers and, with them, the ability of data recipients to be able to match and re-identify individual records.

Data Item Masking:

- Mask the sensitive elements of database records from being accessed, transmitted, displayed, printed or otherwise disclosed or modified.

Technological Reinforcements (Cont'd)

Strong Authentication:

- Strong, reliable methods of authentication are necessary to ensure that only authorized individuals, both internal and external, can access and use the data.

Digital Rights Management (DRM):

- DRM can enforce fine-tuned controls over the use and disclosure of data by others, such as their ability to view, copy, print, or forward. DRMs can even auto-delete data or messages not required beyond a specified time period.

Audit Trails / Electronic Tracking:

- A record of all databases accessed should be kept to help detect, deter, and if necessary, prosecute misuse and abuse after the fact.
- Independent third party audit, attestation, and certification may also be desirable for some companies to credibly demonstrate compliance and earn greater trust.

Privacy and Business

The Bottom Line

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

Ten Reasons for Building Consumer Trust

1. Avoiding damage to your company's and/or brand's reputation;
2. Avoiding penalization by any existing or pending laws;
3. Avoiding civil and class-action lawsuits;
4. Maintaining the balance of monitoring the activities of employees while not harming their morale and productivity;
5. Ensuring the continuation of valuable business relationships by ensuring your company measures up to the privacy standards adopted by strategic partners;
6. Being aware of the privacy laws and customs in other countries;
7. Gaining the trust and confidence of customers so that they will not provide you with false information;
8. Dealing with consumers who expect you to treat their personal information the same way that you would treat your own;
9. Repeat online customers are those that feel assured that shopping online is secure and that their information is protected;
10. Gain and maintain an edge over your competitors through embracing more than just the minimum of laws, regulations and privacy best practices.

— Ann Cavoukian, Ph.D., Tyler Hamilton, *The Privacy Payoff: How Successful Business Build Consumer Trust*, McGraw-Hill Ryerson, 2002, pp. 13-14.

Consumer Choice and Privacy

- There is a strong competitive advantage for businesses to invest in good data privacy and security practices;
- *"There is a significant portion of the population that is becoming concerned about identity theft, and it is influencing their purchasing decisions."*

— Rena Mears, Deloitte & Touche LLP, *Survey Reports An Increase in ID Theft and Decrease in Consumer Confidence*, June 29, 2005

Distrust and Profitability

- Consumer data security breaches are leading to customer revolt and an average cost per incident of $14 million - with costs ranging as high as $50m;
- 20% of consumers immediately terminated their accounts with vendors that lost their information;
- An additional 40% considered taking their business elsewhere after receiving notifications of information mishandling.

— Ponemon Institute, *Lost Customer Information: What Does a Data Breach Cost Companies?*, November 2005.

- *"The increasing incidence of reporting of lost private personal records poses a serious threat to consumer confidence – and to vendor profits, yet it is the right thing to do because it is forcing companies to clean up their acts. Companies are beginning to understand the effect carelessness with data can have on their reputations and their bottom line."*

— Esther Dyson, PGP Business Advisory Board, November 24, 2005.

Costs of A Privacy Breach

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

The Unpredictable Cost of Litigation

- 84 new consumer privacy cases in 2005;
- Since 2000, over **$13 billion** in settlements, judgments and verdicts;
- Highest areas of litigation are spam, data breaches and spyware, accounting for **70%** of cases in 2005.

— Robert R. Belair, *Trends in the Washington Privacy Scene*, Privacy and American Business, January 2006.

FTC Decisions:
BJ's Warehouse Club

- **March 2004**, Millions of dollars of unauthorized purchases were made on customer credit and debit cards after customers had visited BJ's stores;
- **June 2005**, the FTC issued a standing order for 20 years.
- Further, a number of financial institutions have filed lawsuits against BJ's seeking the return of about $13 million in fraudulent purchases and operating expenses in connection with the case.

FTC Decisions: *ChoicePoint*

- **February 2005**, personal financial records of more than **160,000** consumers fraudulently obtained; L.A. police believe that the actual number of persons affected could be **500,000**;
- **January 2006**, ChoicePoint fined $10 million in civil penalties by the FTC, the largest in the commission's history;
- An additional $5 million is to be paid in consumer redress to the FTC to settle charges brought against it;
- *"The message to ChoicePoint and others should be clear: Consumers' private data must be protected from thieves. Data security is critical to consumers, and protecting it is a priority for the FTC, as it should be to every business in America."*

— Deborah Platt Majoras, Chairman of the FTC, January 26, 2006.

IBM Survey on Cybercrime

A Greater Threat Than Physical Crime

- An IBM survey of companies in the healthcare, financial, retail and manufacturing industries reported that nearly **60%** of businesses believe that cybercrime is more costly to them than physical crime;
- **84%** of executives believe that organized criminal groups possessing technical sophistication are replacing lone hackers;
- **74%** perceive that threats to corporate security are now coming from inside the organization;
- While **61%** of executives believe it is the joint responsibility of both the federal and local law enforcement agencies to help combat cybercrime – **53%** of consumers hold themselves most responsible for protecting themselves, while only **15%** felt it was the job of law enforcement agencies.

— IBM, *U.S. Businesses: Cost of Cybercrime Overtakes Physical Crime*, March 2006.

IBM Survey on Cybercrime
Safeguarding

83% of organizations believe they have safeguarded themselves and are responding to the increased threat in a number of ways:

- Upgrading virus software (73%);
- Upgrading their firewalls (69%);
- Implementing intrusion detection/prevention technologies (66%); and
- Implementing vulnerability/patch management systems on their networks (53%).

IBM Survey on Cybercrime
International Comparisons

- Both U.S. and international organizations viewed cybercrime as more of a threat to their organizations than physical crime - 57% of U.S. vs. 58% of international businesses;
- Both groups indicated that loss of revenue (63% U.S. versus 74% international) and loss of current customers (56% U.S. versus 70% international) would have the highest cost impact;
- Damage to brand/reputation is of much higher concern to international businesses than those in the U.S. with 69% for international businesses compared to only 40% of U.S. businesses;
- Conversely, legal fees are considered to be a significant cost in the U.S. (33%) while of less concern internationally (19%).

RFID

Radio Frequency Identification

RFIDs

- Radio Frequency Identification (RFID) is technology that uses devices attached to objects that transmit data to an RFID receiver. An alternative to bar coding that has advantages including data capacity, read/write capability, and no line-of-sight requirements;
- RFID tags contain information about a product, not an individual (e.g., EPC, price, size, colour, manufacture date);
- RFID technologies have great potential to make our lives more convenient, efficient, and safer.

Privacy and RFIDs

- Many consumers perceive RFIDs as a threat to privacy;

Why?

- **Because consumers believe that RFIDs may facilitate tracking:**
  - The ability to track consumers who have purchased a product;
  - The establishment of a widespread surveillance infrastructure;
  - The linking of product information and personal information without consent.

IPC RFID Materials

- *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (February 2004); www.ipc.on.ca/docs/rfid.pdf
- *Guidelines for Using RFIDs in Public Libraries* (June 2004); www.ipc.on.ca/docs/rfid-lib.pdf
- RFID Video, *A Word About RFIDs and Your Privacy in the Retail Sector*, (February 2006).

  www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=19&U_ID=0

Legislation

United States
*Sectoral Laws: A Sample**

- 2006: Financial Data Protection Act, 2005
- 2005: FTC “Disposal Rule”
- 2003: California SB1386
- 2002: Sarbanes-Oxley
- 2000: Children's Online Privacy Protection Act
- 1999: Gramm-Leach-Bliley

* *This list represents only a small sample of sectoral laws in the United States.*

Sarbanes-Oxley

- Sarbanes-Oxley (2002) is a legislative response to corporate mismanagement:
  - Includes enhanced safeguards against conflicts of interest for management;
  - New system of private oversight, public reporting and independence rules for auditors;
  - Audit committees given direct responsibility for overseeing the external audit process;
  - Imposes responsibilities on publicly-traded companies to establish and maintain adequate internal controls over information systems, as well as an assessment of the effectiveness of those internal controls.

Gramm-Leach-Bliley

- Also known as the Financial Services Modernization Act, 1999, this law includes provisions to protect consumers' personal financial information held by financial institutions;

- Significant privacy and security elements for consumers in the *Act* include:
  - Provision of a comprehensive privacy notice upon application and on an annual basis;
  - Provision of a detailed security policy that identifies and assesses the risks that may threaten customer information;
  - Provision of opt-out rights for individuals for any sharing of personal information with non-affiliated third party companies;
  - Implementation of significant security safeguards.

Trend to Short Notices

- Short notices to the public came to be realized as a necessity when legislation governing privacy began to increase, prompting many organizations to accommodate as much of the new regulations as possible into their privacy statements and notices;

"When GLBA and HIPAA were passed, there was a requirement to make these notices even more complete and long. That has resulted in privacy notices that are barely readable and largely ineffective."

— Martin Abrams, Executive Director,
Center for Information and Policy Leadership,
Hunton & Williams LLP, 2004

Benefit of Short Notices

While individuals are the main beneficiaries of improved communication of information about an organization's privacy practices, there are also benefits for organizations:

- To communicate more effectively with the public, allowing for the growth of a relationship based on trust ***through simple understanding;***
- A standardized format could be used globally by an organization to provide for economies of scale.

Global Focus on Short Notices

- **Sydney Data Protection Commissioners' Resolution, 2003:** Emphasized the importance of improving the communication of information in handling and processing personal information; achieving global consistency in communicating this information; improving individuals' understanding and awareness of their rights and choices; and putting an incentive on organizations to improve their information handling processing practices;
- **Berlin Memorandum, 2004:** Recognized that new architecture was needed for privacy notices. In effect, privacy notices should be multi-layered, written in plain language, compliant with relevant law, in a consistent format and contain no more information than individuals can reasonably process;
- **Short Notices, 2005:** Short Notices are a ***must*** in order to comply with Ontario's new PHIPA; Ontario Bar Association worked closely with the IPC to achieve this goal.

European Union Directive

Article 17 of the European Union's Directive on Data Protection:

- When one person or body retains another to process personal data (including the destruction of such data) on its behalf, it must choose one that provides "sufficient guarantees governing the processing to be carried out;"

- Further, such processing of personal data must be governed by "a contract or legal act" that stipulates, among other things, that the person or body processing the data shall act only on instructions from the person or body that retained it.

General Electric
Binding Corporate Rules

General Electric attempts to address privacy on a global basis based on **Binding Corporate Rules (BCR),** which require organizations to have user friendly access to the company's policies as well as an employee code of conduct that addresses privacy;

BCRs are an effective compliance approach because they are:

- Visible to employees;
- User-friendly for data handlers, third parties and employees;
- Obligatory for company entities and employees;
- Harmonized global guidelines ensuring a consistent, strong protection.

Google
A Case for Online Privacy

- The federal government subpoenaed Google to bolster their case for resurrecting the 1998 *Child Online Protection Act*, COPA;
- COPA was struck down in 2004 on free speech grounds argued by the ACLU, EPIC and other groups;
- The government claims it requires the data from Google to prove COPA's constitutionality;
- The original request was for billions of URLs and an entire week's worth of search queries;
- California District Judge, James Ware, ruled that Google must turn over the 50,000 websites, but is not required to turn over the 5,000 search queries which were seen as the most problematic from a privacy perspective.

Solutions

American Institute of Certified Public Accountants/ Canadian Institute of Chartered Accountants – Privacy Framework

- ***AICPA/CICA Privacy Framework,*** Exposure Draft June 3, 2003

  www.aicpa.org/innovation/baas/ewp/privacy_framework

- Set of Generally Accepted Privacy Principles (GAPP) to which a Chartered Account could provide independent attestation;

- Businesses could provide clients with assurance of compliance with privacy standards (e.g. EU Data Protection Directive, Safe Harbor, PIPEDA, GLB, HIPAA, Australian privacy requirements;

- Professor Marilyn Prosch is one of the principle architects of the above framework.

Global Privacy Standard
Values

The objective of the **Global Privacy Standard** is to form a set of universal privacy principles, harmonizing those found in various sets of fair information practices;

- **Existence of Privacy:** An individual possesses a physical, social, and informational identity that relates to his or her private domain;
- **Withholding:** Individuals have the right to withhold some or all of their personal information, as they see fit, from other persons and organizations;
- **Dissemination:** Individuals have the right to disclose some or all of their personal information and to issue constraints on, and vary the use and disclosure of, their personal information;
- **Trusted Usage:** The collection and processing of personal information shall abide by the laws that control dissemination and processing in their respective jurisdictions.

Global Privacy Standard
Scope

The Global Privacy Standard reinforces the mandate of privacy and data protection authorities by:

- **Focusing** attention on fundamental and universal privacy concepts;
- **Widening** current privacy awareness and understanding;
- **Stimulating** public discussion of the effects of new information and communication technologies, systems, standards, social norms, and laws, on privacy; and
- **Encouraging** ways to mitigate threats to privacy.

Identity Metasystem

The Problem

The Internet was built without a way to know who and what you are connecting to:

- Patchwork of identity one-offs;
- Consumers open to “phishing” and “pharming;”
- No use blaming the consumer because there is no framework, no cues and no control;
- Digital identity currently exists in an online world without synergy;
- Securely and reliably identifying and authenticating external customers has always been a major challenge.

Identity Metasystem
The Solution

- Fortunately, there is an emerging "Identity Metasystem" that will allow different identity systems to interconnect and work together in a secure framework;
- Microsoft's new "InfoCard" software will provide tools for users to identify themselves securely to organizations when online, using a minimum of personal information;
- InfoCard will also ensure that users can be confident about the identity of organizations with whom they interact online, helping to reduce the identity theft risks and effects of fraudulent 'phishing' and 'pharming' tactics by imposters;
- Kim Cameron, *The Laws of Identity*, May 2005, www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

Identity Metasystem
The Benefits

- User Control; Empowerment;
- Enables new relationships;
- Increased flexibility; Increased audience;
- Policy, claims transformation enables wide variety of relationships;
- Easy to add support for new technology;
- Simple, safe user experience.

Data Privacy = Good Data Security

Privacy is:

- ***Holistic*: Develop a *culture of privacy*** – involving the entire organization;
- ***Personal*: Consider the individuals' interests;**
- ***Comprehensive*: Privacy enhances security.**

Make Privacy A Corporate Priority

- An effective privacy program needs to be integrated into the corporate culture;
- It is essential that privacy protection become a corporate priority throughout **all** levels of the organization;
- Senior Management and Board of Directors' commitment is critical.

Good Governance:

CICA's 20 Questions

Directors Should Ask About Privacy

1. What personal information (PI) about customers and employees does the organization collect & retain?
2. What PI is used in carrying out business, for example, in sales, marketing, fundraising and customer relations?
3. What PI is obtained from, or disclosed to, affiliates or third parties, for example, in payroll outsourcing?
4. What is the impact of the PIPEDA, and/or provincial or international privacy requirements, on the organization (a legal interpretation may be required)?
5. How does the organization's business plan address the privacy of PI?
6. To what degree is senior management actively involved in the development, implementation and/or promotion of privacy measures within the organization?
7. Has the organization assigned someone (for example, a Chief Privacy Officer) the responsibility for compliance with privacy legislation?
8. Has the designated privacy officer been given clear authority to oversee the organization's information handling practices?
9. Are adequate resources available for developing, implementing and maintaining a privacy compliance system?

Good Governance:

CICA's 20 Questions

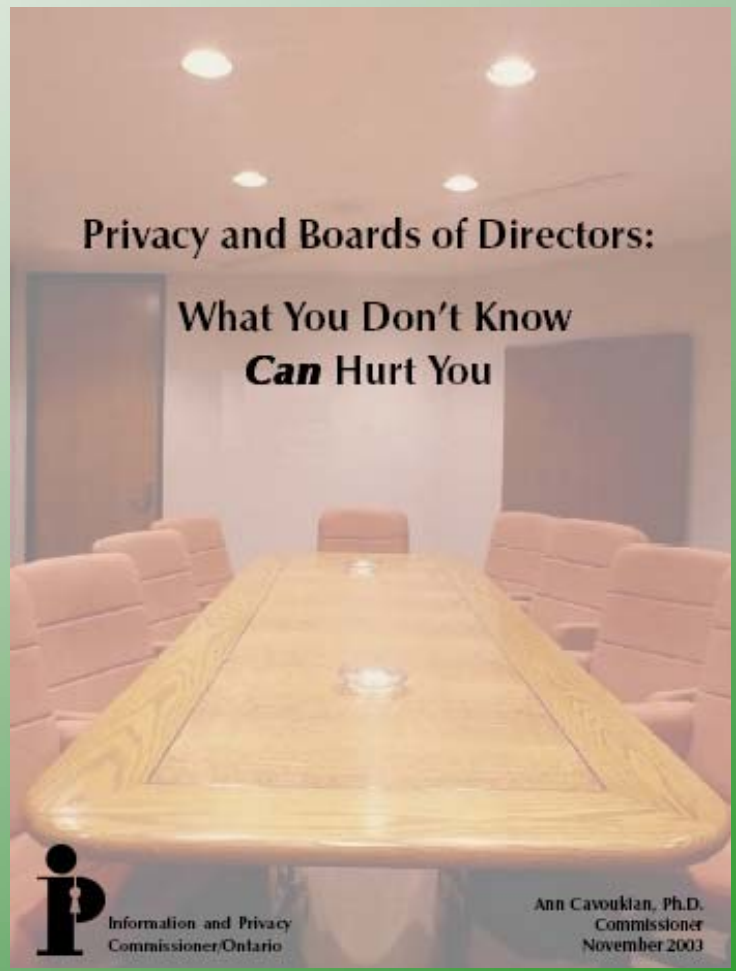
Directors Should Ask About Privacy

10. What privacy policies has the organization established with respect to the collection, use, disclosure and retention of PI?
11. How are the policies and procedures for managing PI communicated to employees?
12. How are employees with access to PI trained in privacy protection?
13. Are the appropriate forms and documents required by the system fully developed?
14. To comply with the organization's established privacy policies, what specific objectives have been established?
15. What are the consequences of not meeting the specific privacy objectives?
16. To what extent have appropriate control measures been identified and implemented?
17. How is the effectiveness of the privacy control measures monitored / reported?
18. What mechanisms are in place to deal effectively with failures to properly apply the organization's established privacy policies and procedures?
19. How would the organization benefit from a comprehensive assessment of the risks, controls and business disclosures associated with PI privacy?
20. Has the organization considered the value-added services available from an independent assurance practitioner with respect to both offline and online privacy?

Good Governance and Privacy

IPC Publication:

- Guidance to corporate directors faced with increasing responsibilities and expectation of openness and transparency;
- Privacy among the key issues that Boards of Directors must address;
- Potential risks if Directors ignore privacy;
- Great benefits to be reaped if privacy included in a company's business plan.



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

Final Thought

"Anyone today who thinks the privacy issue has peaked is greatly mistaken…we are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope."

- Forrester Research, March 5, 2001

How to Contact Us

Commissioner Ann Cavoukian

Information & Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca