

**Privacy:
What You Don't Know As
a Director *Can* Hurt You**

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

November 20, 2003

*Canadian Center for Ethics and Corporate
Policy*





Agenda

- Why directors must pay attention to privacy
- FIPs: a shorthand for information privacy
- Potential risks of failing to address privacy
- Business case for sound privacy practices
- What Board Directors should do to promote privacy compliance



Duties of Directors

- **fiduciary duty** to act in the best interests of the corporation
- **duty to maintain the standard of care** – directors are required to exercise the care, diligence and skill that a “reasonably prudent person” would exercise in comparable circumstances

Canadian Business Corporations Act



View from the U.S.A.

The Sarbanes-Oxley Act (2002)

- Sarbanes-Oxley (2002) is a legislative response to corporate mismanagement (e.g. Enron):
 - 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



Increasing the Risk of a Privacy Meltdown

- information technology – accumulate, link and share massive amounts of personal information
- globalization of the economy – personal information may be stored anywhere in the world, often without any protections
- interconnectivity of businesses – information shared among affiliates and associates
- Web-based delivery of products and services facilitate collection and tracking; disclosures have bigger impact – on a much larger scale



Privacy Debacles – Who's Liable for the Damage?

- Eli Lilly – disclosed e-mail addresses of 600 individuals registered to receive reminders about taking Prozac
- ISM – theft of hard drive with personal information of thousands of Canadians
- California – state personnel database hacked
- Florida – antidepressant users sent unsolicited samples of Prozac



How Can An Organization Protect Privacy?

- implement an internationally recognized privacy standard commonly referred to as “fair information practices”
- fair information practices balance an individual’s right to privacy with an organization’s legitimate need to collect, use and disclose personal information



Fair Information Practices: A Brief History

- *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)*
- *EU Directive on Data Protection* led to expansion of privacy laws in many countries around the world (1995)
- *Canadian Standards Association Model Code for the Protection of Personal Information (1996)*
- *Federal Personal Information Protection and Electronic Documents Act (1999)*



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

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



CSA Model Privacy Code

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





Consequences of Privacy Breaches

- violations of privacy legislation
- damage to an organization's reputation, brand image, and business relationships
- psychological and economic harm to customers
- loss of customer trust and loyalty
- financial losses due to deterioration in data quality and integrity resulting from lack of trust
- loss of market share and drop in stock prices following a “privacy hit” or cancellation or delays in roll out of new products and services due to privacy concerns



Violations of Privacy Legislation

- January 1, 2004 all Canadian organizations will be covered by federal or provincial privacy legislation (Quebec, BC, Alberta will have own)
- legislation will apply to all officers and directors
- Privacy Commissioner may conduct investigation or audit; publicize information about practices
- Privacy Commissioner or complainant may apply for court hearing
- unlimited monetary damages may be awarded to a complainant by courts



Damage to Reputation, Brand Image, and Business Relationships

- media attention or a formal privacy complaint can lead to unwanted scrutiny by advocates
- adverse publicity can affect stock prices and attract shareholder lawsuits if organization is seen as failing to comply with the required standard of care to prevent foreseeable damage
- organizations may be exposed to risk if business partners, agents, and service providers fail to comply with privacy legislation



How to Contain Damage Following A Privacy Breach

- potential damage may be minimized through a **privacy crisis management protocol**
- in the event of a privacy breach, the privacy crisis management protocol should require:
 - Immediate **notification** of Board of Directors
 - notification of individuals whose privacy has been breached so they can take steps to prevent adverse consequences such as identity theft
 - notification of privacy oversight body
 - **Containment**: steps taken to prevent a reoccurrence



Harm to Your Customers

- privacy breaches may expose an organization to customer lawsuits
- class action lawsuits are a growing trend
- in 2001, US based companies forced to pay \$60 million in settlements or judgments, usually for failing to comply with a stated privacy *policy*



Individual Harms

- unwanted intrusions – junk mail, spam, telemarketing
- physical harm – stalkers, abusive former partners, pedophiles, sexual predators, etc.
- psychological harm – stigmatization, discrimination through disclosure of medical and psychiatric conditions, alcohol or drug addiction, etc.
- economic harm – identity theft is the fastest growing crime in North America
- harm may be reduced if privacy crisis management protocol is implemented immediately



Deterioration in Data Quality and Integrity

- accurate, complete and up-to-date information is needed to provide individualized products and services and to make informed business decisions
- fair information practices require that data be kept accurate and generally foster trust
- lack of trust – customers may avoid providing truthful information; withhold consent for use and disclosure



Lack of Trust on the Web

“In 70% of instances where Internet users were asked to provide information in order to access an online informational resource, those users did not pursue the resource because they thought their privacy would be compromised.”

Narrowline Study, 1997



Falsifying Information on the Web

“42.1% have falsified information at one time or another when asked to register at a Web site.”

10th WWW User Survey, October 1998



The Impact of Lack of Trust

“Absent trust, Web consumers seem to be more than willing to upset the marketing apple cart. They refuse to cooperate: 94% have declined to provide any personal information when asked -- and they lie through their teeth.”

Wired Magazine, May 1998



Loss of Market Share and Drop in Stock Prices

- customers can take their business to a competitor with stronger privacy practices
- companies have been forced to withdraw/ delay roll of out products/services due to public outcry and consumer boycotts over perceived privacy invasiveness (e.g, Intel computer chip ID; Gillette RFID tracking)
- delays can open a door for the competition
- retrofitting or redesigning – more expensive than building in privacy up-front: “privacy by design”



Benefits of Strong Privacy Policies and Practices

- strong organizational image and competitive edge
- potential for expansion into jurisdictions requiring adherence to strong standards
- enhanced data quality and integrity fostering better customer services and strategic decision making
- enhanced customer trust and loyalty
- savings in terms of time and money



Sound Privacy Policies Foster Positive Image and Competitive Edge

- 83% of survey respondents would stop doing business with a company entirely if they heard or read that the company misused customer information.

-Harris Interactive Poll, 2002

- “Our research shows that 80% of our customers would walk away if we mishandled their personal information.”

CPO, Royal Bank of Canada, 2003

- sound privacy policies can be thought of as “insurance” for a company’s hard-earned and often costly brand image.



Sound Privacy Policies Allow Business Expansion

- EU Directive prohibits the flow of personal information to non-member countries without adequate privacy safeguards
- lack of privacy protections can impose a non-economic trade barrier to companies that want to do business in jurisdictions with higher privacy standards



Privacy and Customer Loyalty

- trust is the basis for customer loyalty
- an increase in customer retention rates of 5% will increase profits from 25% to 95%
(Frederick Reichheld, *Loyalty Rules!*)
- largely due to low cost of retaining customers compared to the high cost of acquiring new customers
- sound privacy policies are an important part of a good customer retention strategy



A Proactive Approach to Privacy Will Save Time and Money

Save time and money by avoiding:

- law suits initiated by customers, shareholders and business partners
- inquiries and complaints from customers
- investigation or audit by Privacy Commissioner
- inefficiencies resulting from poor information management practices and the retention of inaccurate, incomplete, out-dated information
- failure/delay in the roll out of a new product or service due to privacy concerns
- retrofitting or redesigning a product or services to address privacy concerns



What Should Directors Do?

- Director education is key -- ensure privacy training and some level of expertise on board
- designate at least one senior manager as being accountable for privacy compliance
- make privacy compliance part of management performance evaluation and compensation package
- ask management to undertake privacy self-assessments and privacy audits
- ask management to demonstrate compliance with legislation and best practices in order to reap “bottom line” advantages



AICPA/CICA Privacy Framework

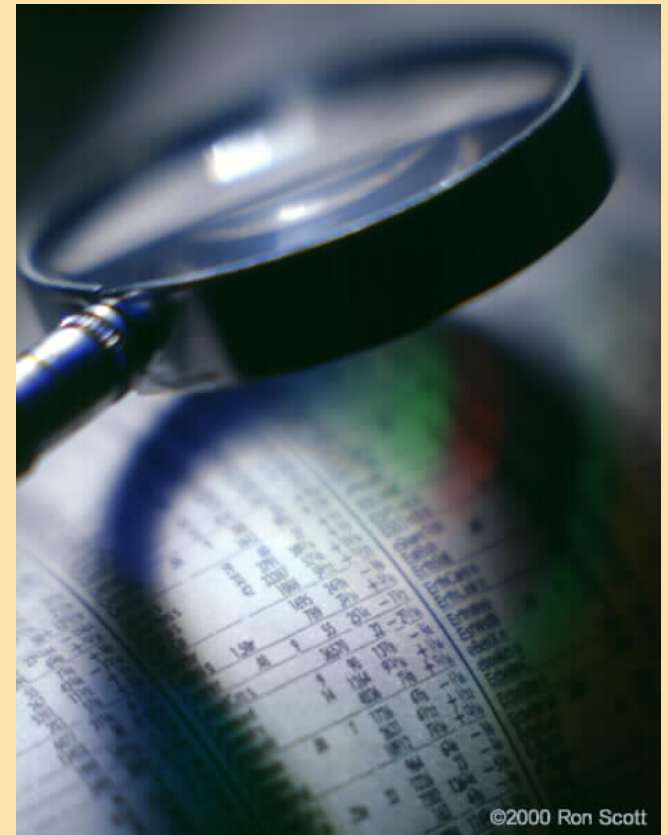
- *Privacy Framework* Exposure Draft June 3, 2003
 - www.cica.ca/privacy
- Set of Generally Accepted Privacy Principles (GAPP) to which a Chartered Account could provide an attestation report
- Business could provide their clients with assurances that it is complying with privacy standards (e.g. EU Data Protection Directive, Safe Harbour, PIPEDA, GLB, HIPAA, Australian privacy requirements)



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

Ann Cavoukian, Ph.D.

Commissioner

80 Bloor Street West, Suite 1700

Toronto, Ontario Canada M5S 2V1

Phone: (416) 326-3333

Web: www.ipc.on.ca

E-mail: commissioner@ipc.on.ca