Make Privacy Work for You:
Turn Promises Into Strategies

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

International Association of Business Communicators

Vancouver, B.C.

June 7, 2006

IPC

Presentation Outline

1. *The Privacy Landscape*
2. *Identity Theft*
3. *Privacy and Business*
4. *Consumer Confidence and Trust*
5. *How the Public Divides on Privacy*
6. *Privacy and Marketing*
7. *Conclusion: Use Privacy to Gain a Competitive Advantage*

IPC

The Privacy Landscape

IPC

The Privacy Landscape

- Growth of Privacy as a Global Issue (EU Directive on Data Protection);
- Exponential growth of personal data collected, transmitted and exploited;
- Consumer Backlash; heightened consumer expectations;
- Convergence of growth in bandwidth, sensors, data storage and computing power.

IPC

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.

IPC

Understanding the Difference: *Privacy and Security*

- While security and privacy share some important common qualities and features, ***security is not privacy*;**
- Privacy relates to the protection of the ***individual****;*
- Security deals with information management practices from a top-down control perspective in an effort to protect company data, processes and systems from attackers;
- IT security professionals often make the mistake of believing that if data can be kept confidential and preserved from corruption, then privacy is guaranteed; ***it is not.***

IPC

The Golden Rules: *Fair Information Practices*

- **Why are you asking?**
  - Collection; purpose specification;
- **How will the information be used?**
  - Primary purpose; use limitation;
- **Any secondary uses?**
  - Notice and consent; prohibition against unauthorized disclosure;
- **Who will be able to see my information?**
  - Restricted access from unauthorized third parties.

IPC

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

IPC

United States
Safe Harbor

Privacy Principles:

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

As of June 1, 2006, there were 950 businesses signed under the Safe Harbor Agreement.

IPC

Identity Theft

IPC

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

IPC

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;

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.

May 2006: *Department of Veterans Affairs* – Theft of 27 million records.

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

IPC

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.

IPC

ChoicePoint

- **February 2005**, in a plot twist taken from a Hollywood movie, criminals were creating false identities to establish accounts with ChoicePoint and then using those accounts to commit identity theft;
- ChoicePoint contacted up 170,000 persons it believed were directly affected but Los Angeles police believe that the actual number of persons affected could be 500,000 or more;
- **January 2006**, in a settlement with the FTC, ChoicePoint agreed to pay $10 million in civil penalties and $5 million in consumer redress in addition to implementing new procedures to ensure that it provides consumer reports only to legitimate businesses and to obtain audits by an independent third-party biennially for the next 20 years.

Full Report: www.ftc.gov/opa/2006/01/choicepoint.htm

IPC

Burglary Leaves Millions at Risk of Identity Theft

- **May 2006**, 27 million U.S. veterans were placed at risk of identity theft after a burglar stole an electronic data file from the home of a Department of Veterans Affairs employee containing **unencrypted** names, birth dates and Social Security numbers; The employee took the information home to work on an ongoing project but without authorization;
- The theft represents the biggest unauthorized disclosure ever of Social Security data, and it could make affected veterans vulnerable to credit card fraud;
- The House Veterans Affairs Committee issued a statement calling on the department to restrict access to sensitive information to essential personnel and to enforce those restrictions;
- The department has sent letters to all of the veterans to notify them that their personal information has been compromised;
- Further, the department will require all employees to complete a computer security training course and conduct an inventory of positions that require access to sensitive data.

IPC

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.

IPC

The Current Privacy Storm
United States

- To date, **thirty-one states** have signed laws that now require consumers to be notified if personal information has been subject to a security breach – **fifteen** other states have such legislation pending;

- Although the new laws are similar to California's SB1386, ***varying state requirements will likely put pressure on Congress to pass a federal bill.***

IPC

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;
- **We place the responsibility for protecting customer’s PII squarely upon business.**

IPC

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.

IPC

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.

IPC

Privacy and Business

IPC

The Bottom Line

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

IPC

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;

IPC

Ten Reasons for Building Consumer Trust (Cont'd)

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

IPC

Privacy is Adversely Affecting E-Commerce

United States: e-commerce sales were only 2.3% of total sales -- $86.3 billion in 2005.

— U.S. Dept. of Commerce Census Bureau, February 2006

Canada: Online sales were 1% of total revenues -- $39.2 billion in 2005.

— Statistics Canada, April 2006

IPC

Taking the Message to Heart

"Smart enterprises know security and privacy are good for business, and yet many companies in Canada and around the world don't take this message to heart."

— Andy Canham, President of Sun Microsystems of Canada, November 22, 2005.

IPC

Consumer Confidence and Trust

IPC

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.

IPC

Lack of Privacy = Lack of Sales

"Consumer privacy apprehensions continue to plague the Web. These fears will hold back roughly **$15 billion** in e-commerce revenue."

— *Forrester Research*

"Privacy and security concerns could cost online sellers almost **$25 billion** by 2006."

— *Jupiter Research*

IPC

The Business Case

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

  — CPO, Royal Bank of Canada

- Nearly 90% of online consumers want the right to control how their personal information is used after it is collected.

IPC

It’s all about Trust

“Trust is more important than ever online … Price does not rule the Web … Trust does.”

— Frederick F. Reichheld,

Loyalty Rules: How Today’s Leaders Build Lasting Relationships

IPC

The High Road

"When customers DO trust an online vendor, they are much more likely to share personal information. This information then enables the company to form a more intimate relationship with its customers."

— Frederick F. Reichheld, *Loyalty Rules: How Today's Leaders Build Lasting Relationships*

IPC

The Low Road

"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 personal information when asked; and they lie through their teeth."

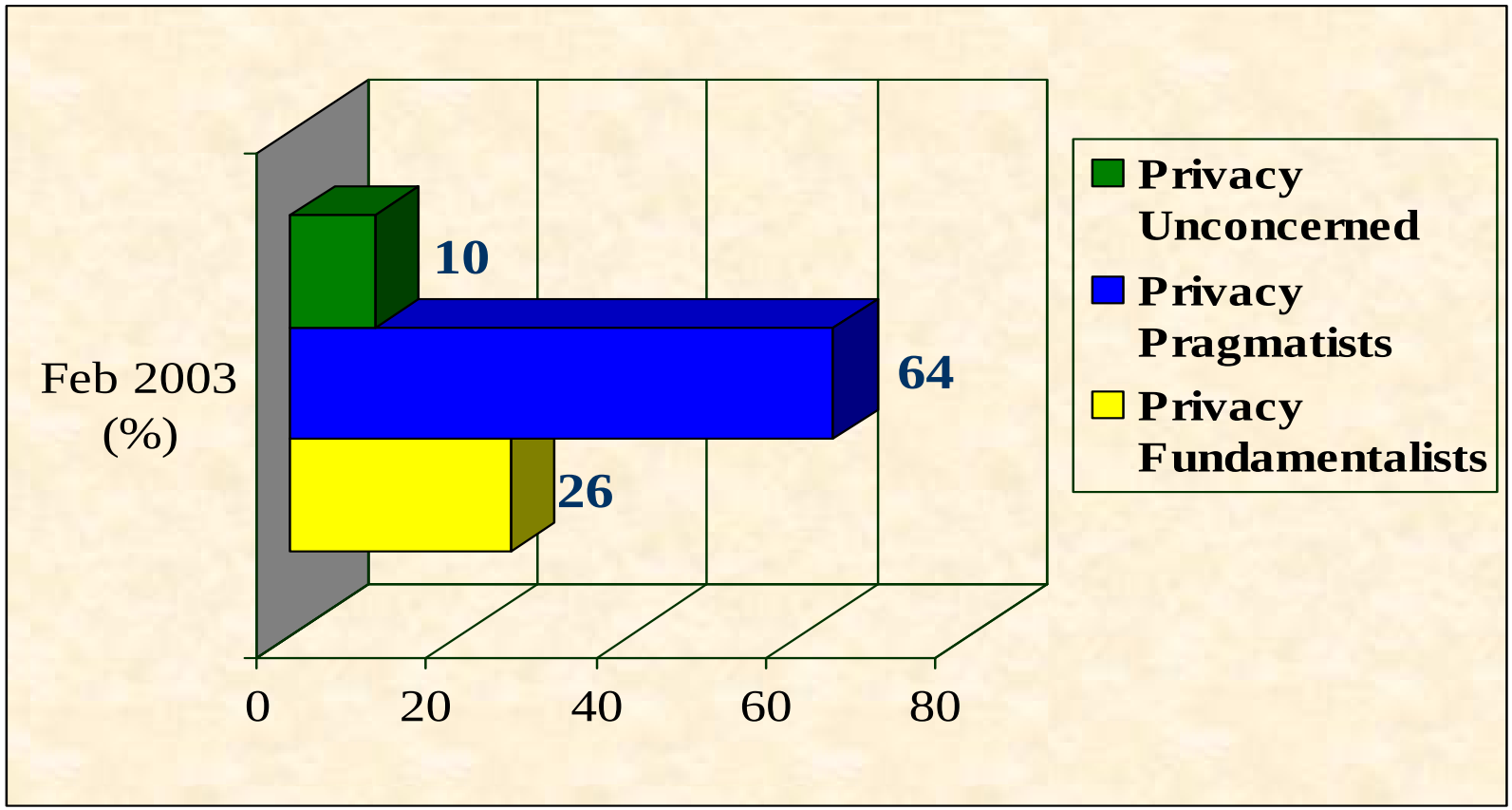
— Wired Magazine

IPC

How the Public Divides on Privacy

IPC

How The Public Divides on Privacy



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

IPC

Privacy and Marketing

IPC

Permission-Based Marketing: *The Personal Touch*

- Essential premise: persuade consumers to ***volunteer*** their attention;
- Puts control in the hands of consumers:
  - Makes consumers ***active*** recipients of marketing information;
  - "Permission marketing is just like dating."

— Seth Godin,

Permission Marketing : Turning Strangers Into Friends and Friends into Customers, Simon & Schuster, 1999.

IPC

Privacy and Customers

"The 1:1 enterprise, operating in an interactive environment, relies not just on information *about* customers, but on information *from* them."

"It is absolutely imperative for the 1:1 enterprise to take into account the issue of protecting individual customer privacy."

— Don Peppers and Martha Rogers, Ph.D

Enterprise One to One: Tools for Competing in the Interactive Age.

IPC

A Privacy-Sensitive Motto for Customer Relations Management

- **The Old Way:**
  - Know everything about your customer;
- **The New Way:**
  - Know everything that your customers **want** you to know;
  - CRM or CMR (customer managed relationship)?
  - Assume nothing – always ask!

IPC

Privacy and CRM

Incorporating Privacy into Marketing and Customer Relationship Management:

- Paper released in May, 2004;
- The result of novel a novel partnership between the Canadian Marketing Association and the IPC;
- CRM and marketing must include privacy to be fully successful.

www.ipc.on.ca/docs/priv-mkt.pdf

IPC

Develop a Corporate Culture of Privacy

- Demonstrate that privacy issues affect everything and everyone;
- Persuade and proselytize every division and employee, leave no stone unturned;
- Focus on partnership development, bring value-added;
- Develop a cross-functional team committed to CPOs mandate.

IPC

Conclusion

- Identity theft is easier than you think – and it's often an inside job;
- Poor information management practices are usually at fault;
- Protecting your customers personal information is ***your business's*** responsibility;
- When faced with a breach, lead with openness and transparency: Contain the damage, then notify affected parties;
- Privacy enhances consumer confidence and trust;
- Use privacy as a tool to gain a ***competitive advantage***;
- Think strategically about privacy – ***it makes good sense – good business sense.***

IPC

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) 326-3333 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

IPC