Identity Theft Could Hit Your Business Next:

How to Protect Your Customers' Privacy

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

BITS Advisory Council

May 16, 2006

IPC

Presentation Outline

1. *Security ≠ Privacy*
2. *Privacy Fair Information Practices*
3. *Identity Theft*
4. *Why Privacy is Good for Business*
5. *Legislation*
6. *Solutions*
7. *Conclusion*

IPC

What is Privacy?

IPC

What Privacy is Not

Security ≠ Privacy

IPC

Understanding the Difference: *Privacy and Security*

- While security and privacy share some important common qualities and features, **security is *not* privacy;**
- Privacy means the protection of the *individual;*
- Security tends to look at 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.

IPC

Fair Information Practices:
A Brief History

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980);
- CSA Model Code for the Protection of Personal Information (1996);
- European Union Directive on Data Protection (1998);
- United States Safe Harbor Agreement (2000).

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* — 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* — Laptop stolen with 196,000 customer files;
Mar 2006: *Georgia Tech Authority* — Hacker theft of 553,000 pension files.

*****For a full chronology of data breaches visit Privacy Rights Clearing House,* 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

Victims of ID Theft: *The Consequences*

- In almost every case, the victim of an identity theft has absolutely no idea they have become a victim until it is far too late;
- Unexpectedly, the victim may find they are denied credit, turned down for a loan, or denied an apartment rental – almost anything that involves a credit or background check;
- "Data rape" leaves victims to spend hundreds of hours, and dollars in repairing the damage;
- Victims typically lose $800 and spend up to two years clearing their names.

— ConsumerReports.org, October 2003.

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

Insider Threat

“In creating large databases, whether for government or corporations, we are opening ourselves to the possibility that the databases will be subverted by attackers.”

— Bruce Schneier, Beyond Fear, 2003

"In the vast majority of cases we investigate, the culprits are current or former employees. They are not hacking into systems using flaws in software. Instead they are using flaws in the security procedures of the company to carry out their attack.“

— Detective Inspector Chris Simpson, London Police, Euro-InfoSec Conference, 2005

IPC

Inside Job

If the Nation's Central Bank Isn't Safe, What Is?

Canada Savings Bonds accounts breached; Cyber-theft limited to 16 accounts, Toronto Star, April 8, 2006;

- The Royal Canadian Mounted Police made two arrests after $100,000 was withdrawn electronically from 16 Canada Savings Bonds accounts;
- In addition to the fraudulent redemption of the bonds, the information was also used to apply for credit cards and cellular phone accounts;
- An **inside job**; the two persons arrested were employed by EDS, a third-party supplier that handles back-office processing for the Canada Savings Bond program.

IPC

Enforcement Case at Japanese Bank

- **February 8, 2006**, an employee of a Mizuho Bank branch was arrested for selling information on 1,251 customers that included account numbers, addresses, telephone numbers, and dates of birth;
- Under Japan's *Personal Information Protection Act* (PIPA), the government can only prosecute enterprises — not individuals;
- **April 25, 2006,** Japan's Financial Services Agency (FSA) issued a warning to Mizuho Bank for failing to set adequate measures to protect customers' information;
- The basis for the enforcement was in violation of Article 20 of the *PIPA* that requires an entity that handles personal information to take appropriate security measures;
- Following the warning, the president and the board members of the bank voted to reduce their salaries by 15 to 30 per cent for a period of 60 days.

— Hunton & Williams, *Japan's FSA Orders Back to Improve Security*, May, 2006.

IPC

Why Privacy is Good for Business

IPC

The Bottom Line

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

IPC

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.

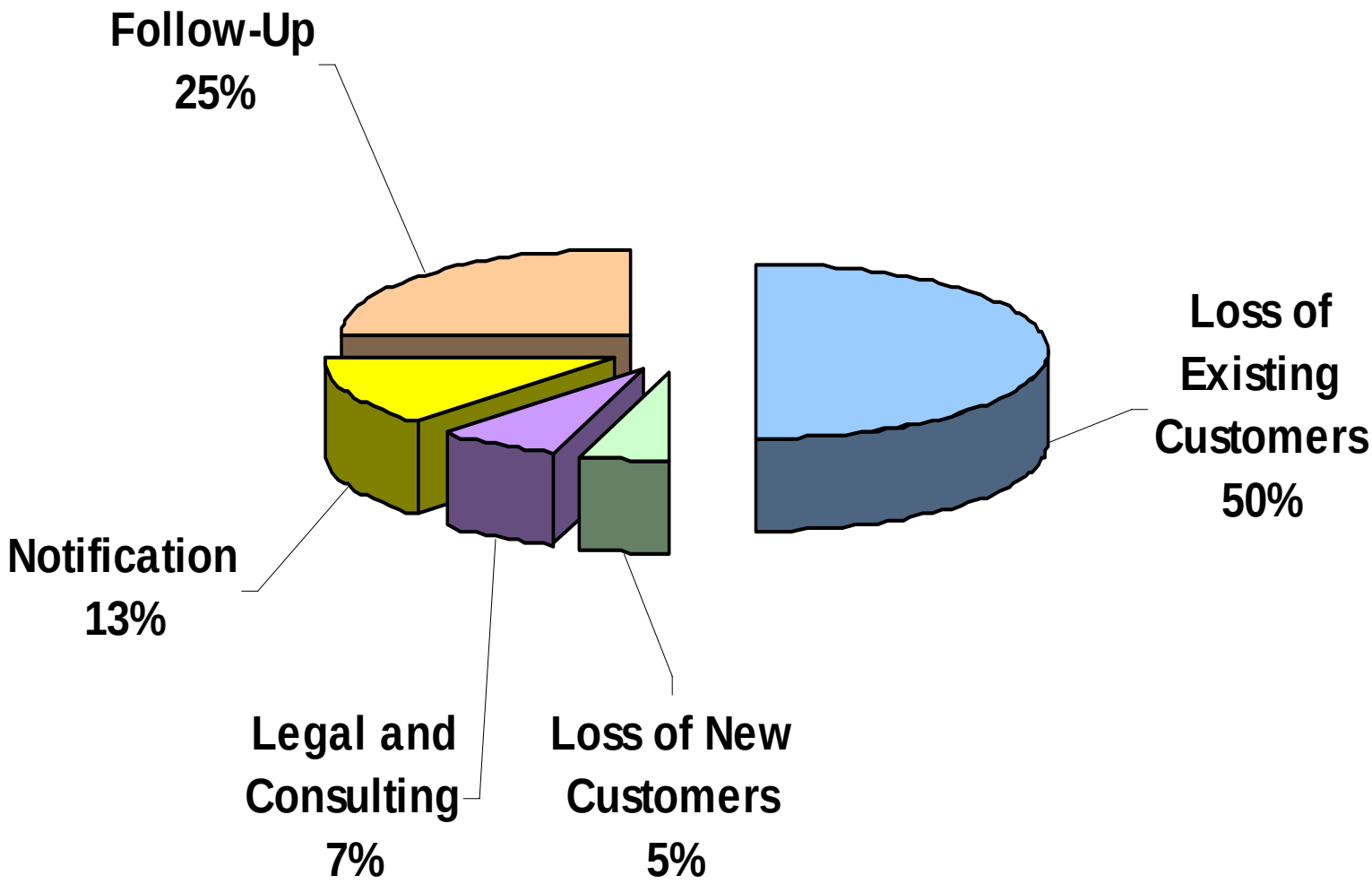
— U.S. Dept. of Commerce Census Bureau, February 2006

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

— Statistics Canada, April 2006

IPC

Costs of a Privacy Breach



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

Legislation

IPC

The Current Privacy Storm
United States

- To date, **twenty-nine states** have signed laws that now require consumers to be notified if personal information has been subject to a security breach – **seventeen** 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

Data-Breach Notification

States Differ on When to Sound the Alarm

- A number of state laws also conflict with each other, define breaches differently and prescribe different thresholds for notification triggers;

Four General Areas:

1. Threshold Notification:

Discretion is allowed regarding whether or not to provide notice, on a harms/severity-of-the-breach basis;

2. California Model:

Notification is required as soon as the security, confidentiality, or integrity of personal information is breached, unless the data are encrypted.

IPC

Data-Breach Notification

States Differ on When to Sound the Alarm

Four General Areas (cont'd):

3. Consumer Reporting Agency Notification:

Some state legislation requires notification of the timing, distribution and content of individual notices to nationwide consumer reporting agencies;

4. Delayed Notification:

Law enforcement intervention permitted to delay providing notice;

IPC

Pending Federal Data-Breach Notification Bills

- **H.R. 3997 - *Financial Data Protection Act*:**

  Notification to consumers if "information is reasonably likely to have been or to be misused in a manner causing substantial harm or inconvenience" to commit identity theft or make fraudulent transactions;
- **H. R. 4127- *Data Accountability and Trust Act*:**

  Notification required unless "no reasonable risk of identity theft, fraud, or other unlawful conduct;"
- **S.1789 - *Personal Data Privacy and Security Act*:**

  Notification of breach not required if there is "no significant risk" that it has or will result in harm;
- **S.1332 - *Personal Data Privacy and Security Act*:**

  Notification of breach not required if "de minimis" risk of harm;
- **S.1408 - *Identity Theft Protection Act*:**

  Notice required if breach creates a "reasonable risk of identity theft", taking into account whether data is in the possession of a third party "likely to commit identity theft;"
- **S.1326 - *Notification of Risk to Personal Data Act:***

  Notification if breach results in "significant risk of identity theft."

* *The above pending bills are designed to pre-empt state laws.*

IPC

The Debate Over Notification
What Consumers Think

- 82% of consumers believe that it is **always** necessary for an organization to report a breach even if there is no imminent threat;

  — Ponemon Institute, *National Survey on Data Security Breach Notification.*

- According to ID Analytics' National Data Breach Analysis, early notification of breached personal information may significantly lower misuse rates;

- There was strong evidence that once a privacy breach was made public (notice of breach), the misuse of the stolen data dropped significantly;

- This suggests that breach notification could serve as a deterrent.

IPC

Solutions

IPC

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.***

IPC

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.

IPC

Technological Reinforcements (Cont'd)

Data Item Masking:

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

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.

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.

IPC

Privacy Breach Protocol

- **Containment:** *Identify the scope of the potential breach and take steps to contain it;*
- **Notification:** *Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly;*
- **Investigation:** *Conduct an internal investigation into the matter, linked to the IPC's investigation and with law enforcement if so required;*
- **Remediation:** *Address the situation on a systemic basis where program or institution-wide procedures warrant review;*

IPC

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.

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*** 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 to gain a competitive advantage;
- Think strategically about privacy – ***it makes good sense – good business sense.***

IPC

How to Contact Us

Commissioner Ann Cavoukian

Information and Privacy Commissioner of 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

IPC