Identity Theft Could Hit Your Business Next:

How to Protect Your Customers' Privacy

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

BITs- Identity Theft Working Group

January 5, 2006

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
- The Canadian offices of Equifax and TransUnion credit bureaus have reported that they receive approximately 1,400 to 1,800 identity theft complaints per month.

Identity Theft is 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.

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.

Consumer Education and Awareness Efforts

- The growing epidemic of identity theft has prompted consumer groups, government agencies, and businesses organizations to introduce consumer education and awareness efforts and to provide some measure of support for victims and others at risk;

- The advice typically takes two forms:
  1. A helpful collection of advice and tips on how to minimize the risk of becoming a victim; and

  2. advice and resources on what to do, where to go, and who to contact after becoming a victim.

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.**

The Real Problem

- Poor information management practices relating to data storage and retention, coupled with the explosive collection of personally identifiable information;

- Massive amounts of personal information retained in largely unencrypted databases – in clear view – of both insiders and outsiders alike.

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

Approximately 80% of all computer and Internet related crimes are committed by insiders.

— CSI/FBI 2003 Computer Crime and Security Survey

Outbreak of Major Privacy Breaches

- **November 2004:** *ChoicePoint* — Identity theft involving 145,000 persons;
- **December 2004:** *Bank of America* — 1.2 million records misplaced;
- **January 2005:** *HSBC* — 180,000 MasterCard records stolen;
- **February 2005:** *Ameritrade* — 200,000 customer files lost;
- **March 2005:** *LexisNexis* — Identity theft of 32,000 records;
- **March 2005:** *DSW Inc* — Hacker theft of 103 credit card numbers;
- **March 2005:** *Boston College* — Theft of 120,000 alumni donor records;
- **April 2005:** *TimeWarner* — Lost files on 600,000 employees;
- **June 2005:** *Citibank* — Lost files on almost 4 million customers;
- **June 2005:** *CardSystems* — Hacker theft of 40 million Visa and MasterCard credit records.

Major Privacy Breach at Boeing

- Highly sensitive personal data on 161,000 Boeing workers went missing after the theft of a company desktop computer;
- The data included extremely sensitive information: names and Social Security numbers, and in some cases, birth dates and banking information.

— David Bowermaster, *PC stolen from Boeing packed with employees' personal data*, Seattle Times, November 19, 2005.

Consumer Data
Cheap but Valuable

- Companies are increasingly collecting personal data from third parties;

The danger?

- *These large databases are held by third parties that have no direct relationship with the people whose information they possess, nor any obligation to provide data access or correction to those persons;*

- This new “infomediary” industry of data brokers is estimated to be worth billions annually;

- The growth of these digital files has become the subject of intense debate about regulatory oversight.

The Coming Privacy Storm

- To date, **twenty-two states** have signed laws that now require consumers to be notified if personal information has been subject to a security breach – a further **thirteen states** 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"*
- August 2005, *SB 1048* – Federal Bill Introduced: "Identity Theft Protection Act."

Data Assets = Data Risks and Liabilities

- The lack of compelling risk and liability for businesses has led speculation that organizations lack strong economic incentives to invest in good data privacy and security practices;
- Further, if the expense of dealing with privacy breaches is minimal compared to the overall bottom line, then fraud and identity theft may be tolerated as the "*cost of doing business;*"
- This is unacceptable if you put your customers first.

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

The Bottom Line

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

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.

Distrust and Profitability

- ***Distrust can have a potentially devastating impact on profitability:***

- **45%** of respondents said there is at least one retail business that they trusted at one time, but no longer trust;

- **94%** said they spent less money with that company, resulting in an average **87%** decrease in spending by that group.

— Yankelovich Study, June 2004

Consumer Trust Is the Key

A simple fact about online behavior:

- Increased trust online breeds 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.

Protecting Personal Information: *An Issue of Vital Importance*

- Four out of five people are concerned about how their finances or health and safety will be affected if their personal data falls into the wrong hands;

- A survey conducted in the U.K. by SMSR Ltd, showed that protecting personal information is now regarded as the third most socially important issue, (coming behind crime prevention and improving education standards).

— Outlaw.com, *Users don't trust websites with personal info,* November 17, 2005.

The Unpredictable Cost: *Litigation*

- *Since 2000*, **182** cases of consumer privacy litigation have been brought against **234** corporate defendants, with **$160 million** paid out in damages.

  - **$52.5m** to the Federal Trade Commission
  - **$39.7m** to state regulators
  - **$32.3m** to private individuals
  - **$28.4m** to private class action
  - **$6.9m** to various federal agencies

— Privacy & American Business, *Consumer Privacy Litigation Report*, 2004

Using Privacy to Gain Competitive Advantage

"How can this legal problem create an opportunity to gain an advantage over one's competitor?"

— George J. Siedel, *Using the Law for Competitive Advantage*, Jossey-Bass, March 2002.

- The answer lies, in part, in adopting comprehensive data privacy practices that can build enduring trust and loyalty.

Fair Information Practices

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

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.

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.***

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.

Crisis Management

Privacy Breach Protocol:

- **Containment:** Identify the scope of the potential breach and take immediate steps to contain it.
- **Notification:** Identify those individuals whose privacy was breached and notify them accordingly.
- **Informing:** Ensure appropriate staff within your organization are immediately notified of the breach.
- **Investigation:** Conduct an internal investigation into the matter, linked to any external investigation.
- **Improving Practices:** Address the situation on a systemic basis. In some cases, program-wide or institution-wide procedures may warrant a review.

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.

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

Web: www.ipc.on.ca

E-mail: commissioner@ipc.on.ca