Privacy and Information Security:
Protecting Your Customers, Protecting Your Business

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Presentation to Fogler, Rubinoff

May 25, 2006

IPC

Presentation Outline

1. **The Privacy Landscape**
   - *Private and Public Sector Laws*
   - *Canada, the U.S., Europe, APEC*
2. **Privacy "101"**
   - *Privacy ≠ Security*
   - *Fair Information Practices*
   - *Use Limitation Principle*
3. **The Stikeman Decision**
   - *What Went Wrong*
   - *Reporting Requirement under SEDAR*
   - *Privacy **Must** Be On Your Radar Screen*
4. **Why Privacy is Good for Business**
   - *Treat Privacy as a Business Issue, Not a Compliance Issue*
   - *Think Strategically: Privacy as a Business Strategy*
   - *Steps Companies Should be Taking Now*
5. **Conclusion**

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; distrust of online activities;
- Convergence of growth in bandwidth, sensors, data storage and computing power.

IPC

Privacy Laws
Canada, United States and Europe

Canada:
Public sector privacy laws: federal, provincial and municipal;
Private sector privacy laws: (Federal) *Personal Information Protection and Electronic Documents Act (PIPEDA)*;
Provincial: Quebec, British Columbia, Alberta;

United States:
Federal public sector *Privacy Act;*
Sectoral privacy laws;
Safe Harbor Agreement;

Europe:
Both private and public sector privacy laws;
- European Directive on Data Protection.

IPC

Canada
Private Sector: PIPEDA

As of 2004, the federal *Personal Information Protection and Electronic Documents Act* applies to:

- all personal information collected, used or disclosed in the course of commercial activities by provincially or federally regulated organizations;
- unless a substantially similar provincial privacy law is in force.

IPC

Provincial Private-Sector Privacy Laws

Québec: *Act respecting the protection of personal information in the private sector;*

B.C.: *Personal Information Protection Act;*

Alberta: *Personal Information Protection Act;*

Ontario: *Personal Health Information Protection Act.*

IPC

United States
*Sectoral Laws: A Sample**

- 2002: Sarbanes-Oxley
- 2000: Children's Online Privacy Protection Act
- 1999: Gramm-Leach-Bliley
- 1996: Health Insurance Portability and Accountability Act
- 1988: Video Privacy Protection Act
- 1986: Electronic Communications Privacy Act

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

IPC

Privacy "101"

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 relates to a broader set of protections involving the protection of the individual – ***personal control****;*
- Security involves organizational control, attempting to protect company data, processes and systems from external attacks;
- 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

Information Privacy Defined

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

IPC

Fair Information Practices:
A Brief History

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980);
- European Union Directive on Data Protection (1995/1998);
- CSA Model Code for the Protection of Personal Information (1996);
- United States Safe Harbor Agreement (2000).

IPC

Summary of 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

Use Limitation Principle

Use Limitation Principle:

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:

i. with the consent of the data subject; or

ii. by the authority of law.

- OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

IPC

The Ten Commandments

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

IPC

The Ten Commandments

4. **Limiting Collection:**
    - collect only the information required for the identified [primary] purpose;
5. **Limiting Use, Disclosure, Retention:**
    - consent of individual required for all other [secondary] purposes;
6. **Accuracy:**
    - keep information as accurate and up-to-date, as necessary for the identified purpose;
7. **Safeguards:**
    - protection and security required, appropriate to the sensitivity of the information;

IPC

The Ten Commandments

8. **Openness:**
   - policies and other information about the management of personal information should be made 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.

IPC

"This Will Become Known as the Stikemans Decision"

— Michael Geist, Professor of Law,
Research Chair of Internet and E-commerce Law at the University of Ottawa,
Globe and Mail, July 20, 2005.

IPC

The Stikemans Decision

The Globe and Mail
Wednesday, July 20, 2005
B7

Firms get wrists slapped over privacy breach

Filing electronic data fraught with legal danger

By BEPPI CROSARIOL

Canadian lawyers got a painful lesson about the legal dangers of filing electronic data when the Alberta Privacy Commissioner's office rebuked two respected firms last week for publishing personal employee information on a public website.

Stikeman Elliott LLP of Toronto and Montreal and Shtabsky & Tussman LLP of Edmonton were singled out for disclosing home addresses and social insurance numbers in connection with a complex corporate buyout of nine oil field services companies by Builders Energy Services Ltd. of Calgary.

The case, the first violation known to involve law firms, highlights the challenge of protecting personal information in the age of the Internet, as well as the vigour with which governments are extending the long arm of Canada's new privacy laws.

The Stikemans Decision (Cont'd)

- ***July 2005***, a privacy investigation conducted by Alberta Privacy Commissioner, Frank Work, found that two law firms and their corporate clients had breached Alberta's *Personal Information Protection Act* (PIPA) during the course of a routine transaction;

- At issue was the disclosure of employees' personal information – their home addresses and social insurance numbers – which were posted onto the publicly accessible SEDAR website;

- The Commissioner reserved his strongest censure for the two law firms involved, finding that both Stikemans and Shtabsky & Tussman had not exercised adequate diligence in the handling of personal information.

IPC

The Stikemans Decision
Commissioner's Comments

"It is unclear whether anyone at [Shtabsky & Tussman and Stikemans] reviewed the contents of the schedule…"

— Frank Work, Alberta Privacy Commissioner.

IPC

The Stikemans Decision

Commissioner's Comments (cont'd)

"We suggest generally that [Stikemans and Shtabsky & Tussman] and other law firms, have shown a lack of attention to the impact of privacy laws on the myriad legal processes involving the collection, use and disclosure of personal information, including client information and third party information that are common in the type of work they perform on behalf of their clients."

— Frank Work, Alberta Privacy Commissioner.

IPC

The Stikemans Decision
SEDAR

- SEDAR (System for Electronic Document Analysis and Retrieval) is the system used for electronically filing most securities-related information with Canadian securities regulatory authorities (provincial securities commissions).
- SEDAR used where securities legislation requires that a document be filed; it applies to any documents listed in a national instrument or "rule" (NI 13-101);
- SEDAR developed for Canadian Securities Administrators:
  - Facilitates the electronic filing of securities information as required by the securities regulatory agencies in Canada;
  - Allows for the public dissemination of Canadian securities information collected in the securities filing process; and
  - Provides electronic communication between electronic filers, agents and securities regulatory agencies.

IPC

Posting of Personal Information on SEDAR

- In Ontario, there is a rule under the Securities Act requiring the posting of *material contracts* on SEDAR, which is accessible to the public (NI 13-101 and Reg. 1015);
- However, there is no specific provision in the Ontario Securities Act explicitly requiring the posting any personal information contained in the *schedules* attached to material contracts (i.e. such as employee SINs and home addresses).

IPC

Posting of Personal Information on SEDAR (Cont'd)

- S. 140(2) of Ontario's Securities Act, permits the OSC to exempt personal information from its electronic filing requirements if the desirability of avoiding disclosure outweighs the desirability of public disclosure.
- This exemption of personal information from public disclosure is reinforced by several OSC rules and policies (i.e. NI 13-101, NI 51-102);

IPC

Privacy Protective Approach

Prudent companies and prudent lawyers representing such companies should consider taking the following approach:

a) avoid putting any unnecessary personal information in the schedules attached to material contracts to be posted on SEDAR or other documents required to be filed under the *Securities Act*; and

b) ask the securities commission (OSC) to exempt personal information under s.140(2) of the *Securities Act* from disclosure either in a schedule to a material contract or other document required to be filed under the *Securities Act*.

IPC

The Problem

- No apparent understanding of what **not** to disclose, and in this case, what not to post publicly on a Web site;
- No apparent distinction drawn between personal information and business (non-personal) information.

IPC

Post Mortem:
What Went Wrong

Privacy Was Lost in the Hierarchy of Compliance:

The observance of privacy laws was eclipsed by the parties' narrow focus on complying with the more onerous, complex and pressing regime under securities law;

Privacy was a Casualty of "Inadvertence:"

The offending information was neither requested by the parties nor reviewed by the law firms. Through "inadvertence," the offending schedule was improperly disclosed not once but **twice**, finding its way onto the Internet. Simply put, no one seemed to turn their minds to existing privacy obligations;

Reliance on Other Parties' Privacy Compliance:

Both Purchaser and Vendor Companies relied, reasonably, on their counsel. Stikemans relied on the representation that the Purchaser was in material compliance with all applicable laws and that its client had signed-off on the schedules. The parties seemed to assume that others compliance would stand-in for their own. In the end, no one identified a potential privacy breach and all four parties were found accountable under the Act.

IPC

Why Privacy is Good for 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

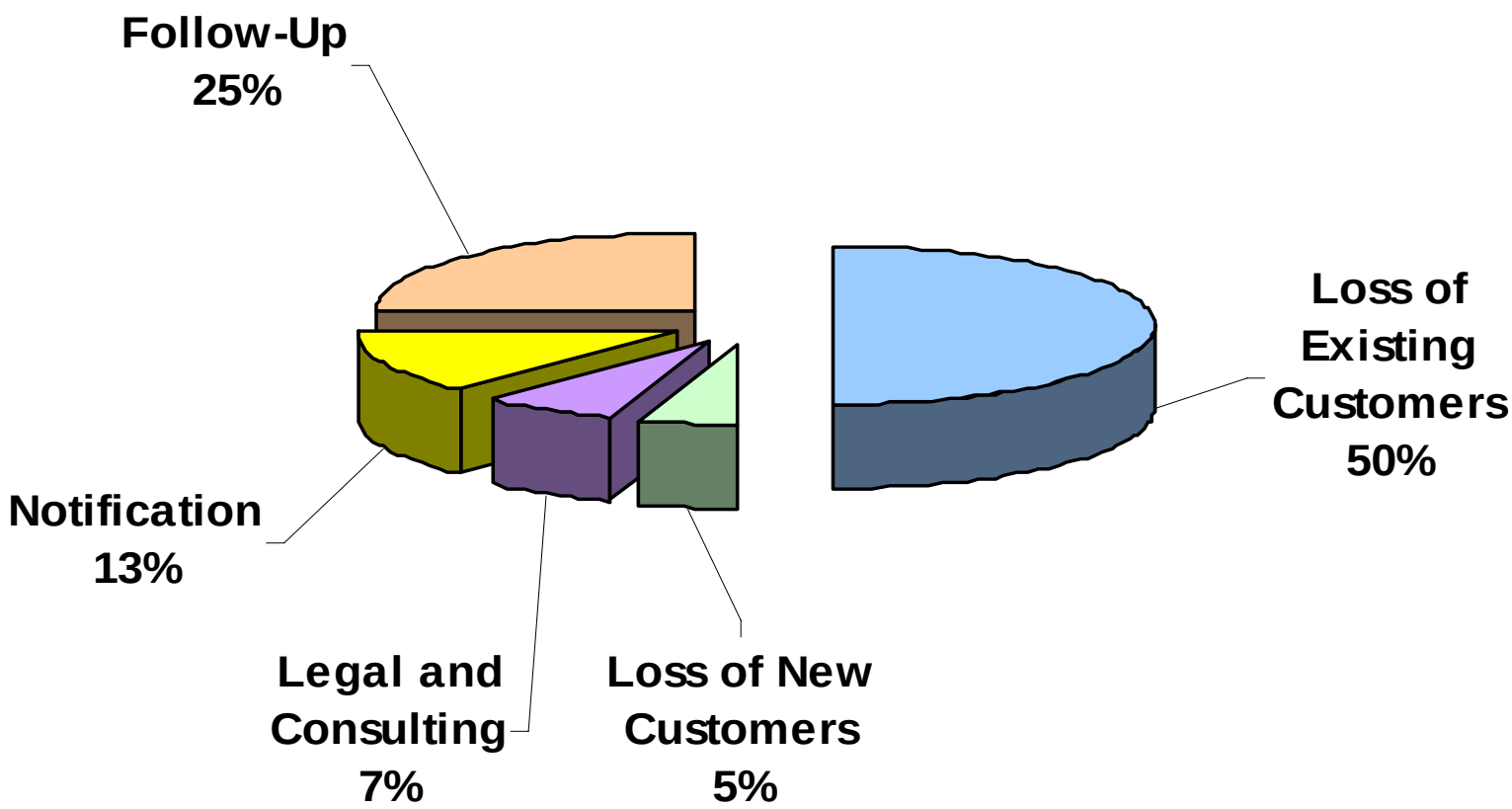
Ten Reasons for Building Consumer Trust (Cont'd)

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 who feel assured that shopping online is secure and 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.

IPC

Costs of a Privacy Breach



Consumer data security breaches are leading to customer revolt and an average cost per incident of $14 million -- with costs ranging as high as $50 million.

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

Make Privacy a Business Asset

- Gain a competitive advantage;
- Enhance trust and consumer confidence;
- Keep existing customers – attract new ones;
- Minimize the risk of a privacy breach and the high costs associated with them.

IPC

Where To Start:
Steps Companies Should Take Now

- Appoint a privacy officer; form a multi-departmental privacy team – build a privacy mindset;
- Develop a privacy policy that closely reflects Fair Information Practices and compliance with relevant privacy laws;
- Train all staff and **re-train** on a regular basis;
- Ingrain the practice of treating "personally identifiable information" differently from business (non-personal) information.

IPC

Assist Your Clients to Develop A Privacy Plan

- Complying with privacy principles may require changes to your clients' personal information management practices;
- Your clients must:
  - Understand and follow privacy principles;
  - Identify company personal information holdings;
  - Assess the impact of privacy principles on operations and align information practices; and
  - Design or change existing information management systems.
- Train staff, re-train staff – an on-going process;
- Test and evaluate systems and processes;
- Create or revise policies, procedures and practices;
- Develop or revise forms and communications material;
- Redraft contracts with agents/suppliers for compliance;
- Inform the public and educate customers – ***use short notices!***

IPC

Alberta Commissioner's Recommendations in the Stikeman Decision

- In-house privacy training for all lawyers and staff;
- Continuing legal education in the area of privacy;
- Review of processes on business transactions where personal information is involved;
- Appoint a privacy officer and implement a corporate privacy policy.

IPC

Make Privacy a Corporate Priority

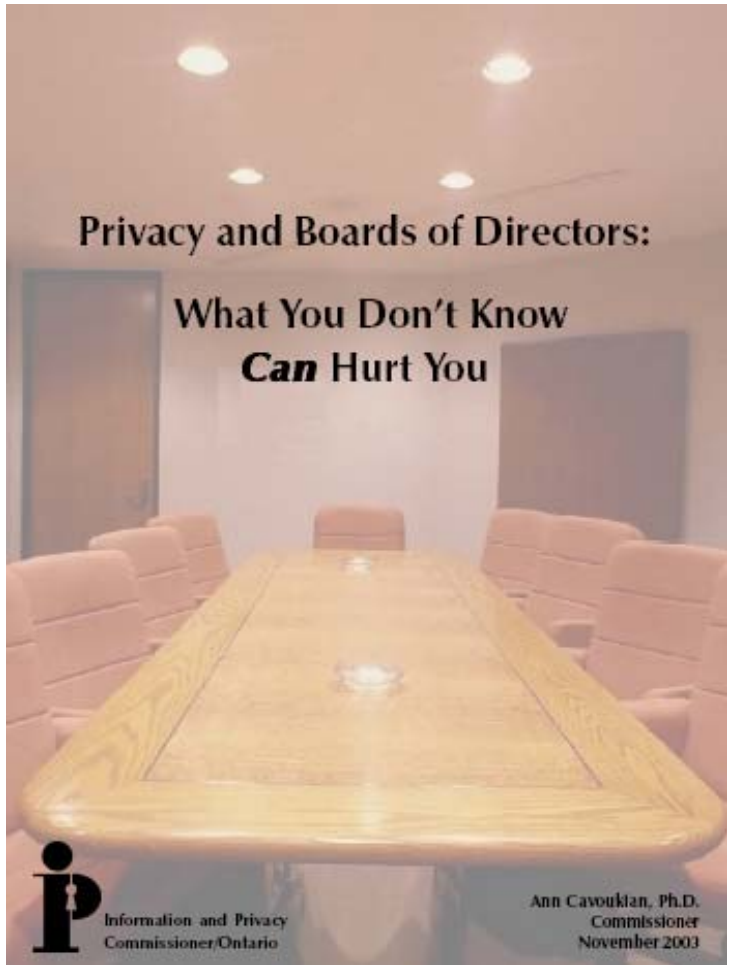
- An effective privacy program needs to be integrated into the corporate culture;
- It is essential that privacy protection become a corporate priority throughout **all** levels of the organization;
- Senior Management and Board of Directors' commitment is critical.

IPC

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

IPC

Conclusion

- Privacy **must** be on your radar screen;
- Both risk aversion (complying with relevant legislation), and attracting opportunity (gaining competitive advantage) come into play;
- The Stikeman decision illustrates this point very clearly – you **must** be aware of any personal information, and protect it from unnecessary disclosure;
- Education is key: train your staff (and your Board), and do it regularly – at a minimum, on an annual basis.

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

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

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 names, birth dates and Social Security numbers;
- The employee took the information home to work on an ongoing project but without any authorization;
- The theft represents the biggest unauthorized disclosure ever of Social Security data, and could make affected veterans vulnerable to credit card fraud or identity theft;
- Democrats on 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

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 Publication. *Identity Theft Revisited: Security is Not Enough*, www.ipc.on.ca/userfiles/page_attachments/idtheft-revisit.pdf

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

Privacy Breach Protocol
Alert Your Incident Response Team

- **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

FTC Decisions

- **ChoicePoint — *January, 2006,*** charged with violating consumers' privacy rights and federal laws by compromising personal financial records of more than 163,000 consumers by not having reasonable procedures to screen prospective subscribers, and turning over consumers' sensitive personal information to subscribers whose applications raised obvious "red flags."

- The settlement requires ChoicePoint to pay $15 million in fines and to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes in addition to establishing and maintaining a comprehensive information security program with independent third-party audits every other year until 2026.

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

IPC

FTC Decisions (Cont'd)

- **Cardsystems — *February, 2006,*** found to be retaining customer information — *in direct contravention of their contract with Visa and MasterCard* — and storing it in a way that put 40 million consumers' financial information at risk;
- The settlement requires CardSystems to implement a comprehensive information security program and obtain audits by an independent third-party security professional every other year for 20 years.

  Full Report: www.ftc.gov/opa/2006/02/cardsystems_r.htm
- **DSW — *December, 2005,*** data-security failure allowed hackers to gain access to the sensitive credit card, debit card, and checking account information of more than 1.4 million customers;
- The settlement requires DSW to implement a comprehensive information-security program and obtain audits by an independent third-party security professional every other year for 20 years.

  Full Report: www.ftc.gov/opa/2005/12/dsw.htm

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

Data-Breach Notification

States Differ on When to Sound the Alarm

State laws conflict, define breaches differently, and prescribe different thresholds for notification;

Three 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 personal information is breached, unless the data are encrypted;

3. Consumer Reporting Agency Notification:

Some state legislation requires notification to nationwide consumer reporting agencies.

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

Debate Over Notification

- Consensus is elusive on when companies should be required to notify consumers that their information has been exposed during a breach;
- Kirk M. Herath, Chief Privacy Officer and Associate General Counsel for Nationwide Insurance Companies said the notification standard should be set to reflect when there is "a clear risk of danger to the consumer;"
- Kirk J. Nahra, a partner at Wiley Rein &Fielding LLP, adds that there is little to be gained by "over-notification" of consumers;
- However, many disagree arguing that companies should not control under what circumstances and when consumers should be notified of a breach or potential harm.

— Jaikumar Vijayan, *Breach notification laws: When should companies tell?,* ComputerWorld, March 2, 2006.

IPC

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

Conclusion

- 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