

The Business Privacy Landscape in Canada: Implications for Data Systems

**Ann Cavoukian, Ph.D.
Information & Privacy Commissioner/Ontario**

IBM Almaden Research Center

April 9, 2003





Industry Canada's View of Data Transfers Between Countries

The transfer of data between countries is a cornerstone of electronic commerce and relies on the existence of agreed-upon rules for the protection of personal information, which apply in and between national jurisdictions.

Industry Canada

http://com-e.ic.gc.ca/english/privacy/article_29.html



Canada's Private Sector Privacy Legislation

In April, 2000 the
*Personal Information Protection and
Electronic Documents Act (PIPEDA)*
became law in Canada.



Scope of PIPEDA

- Federally regulated businesses subject to law
January 1, 2001
- Medical information that is federally regulated
subject to law January 1, 2002
- All other businesses covered **January 1, 2004**
- Provinces may enact “substantially similar”
legislation



The View from the Provinces

- Quebec has private sector privacy legislation
- British Columbia and Alberta to introduce similar private sector privacy bills
- Rest of Canada, including Ontario, to be subject to *PIPEDA*



PIPEDA Approach

- Based on Canadian Standards Association *Model Code for protection of personal information* (CSA Code)
- CSA Code based on the 8 principles of the OECD guidelines: Fair Information Practices
- PIPEDA establishes mandatory obligations and enforcement mechanisms



CSA Code Principles (10 principles)

- Accountability
- Identifying Purposes
- Consent
- Limited Collection
- Limited Use,
Disclosure &
Retention
- Accuracy of data
- Security Safeguards
- Openness
- Individual Access
- Challenge
Compliance



CSA Privacy Principles (1)

➤ **Accountability**

- For personal information
- Designate an individual(s) accountable for compliance

➤ **Identifying Purposes**

- Purpose of collection must be clear at or before time of collection

➤ **Consent**

- Individual has to give consent to collection, use, disclosure of personal information



CSA Privacy Principles (2)

➤ **Limiting Collection**

- Collect only information required for the identified purpose and information shall be collected by fair and lawful means

➤ **Limiting Use, Disclosure, Retention**

- Consent of individual required for other purposes

➤ **Accuracy**

- Keep as accurate and up-to-date as necessary for identified purpose

➤ **Safeguards**

- Protection and security required appropriate to the sensitivity of the information



CSA Privacy Principles (3)

➤ Openness

- Policies and information about the management of personal information should be readily available

➤ Individual Access

- Upon request, an individual shall be informed of the existence, use and disclosure of her personal information and be given access to that information, challenge its accuracy and completeness and have it amended as appropriate

➤ Challenging Compliance

- Ability to challenge all practices in accord with the above principles to the accountable body in the organization



Commissioner's Powers

- Under *PIPEDA*, the Privacy Commissioner:
 - May investigate complaints and conduct audits;
 - Has full array of investigative powers
 - May take matters to federal court
 - Conduct research into privacy matters
 - Promote greater awareness and understanding of privacy issues



Enforcement

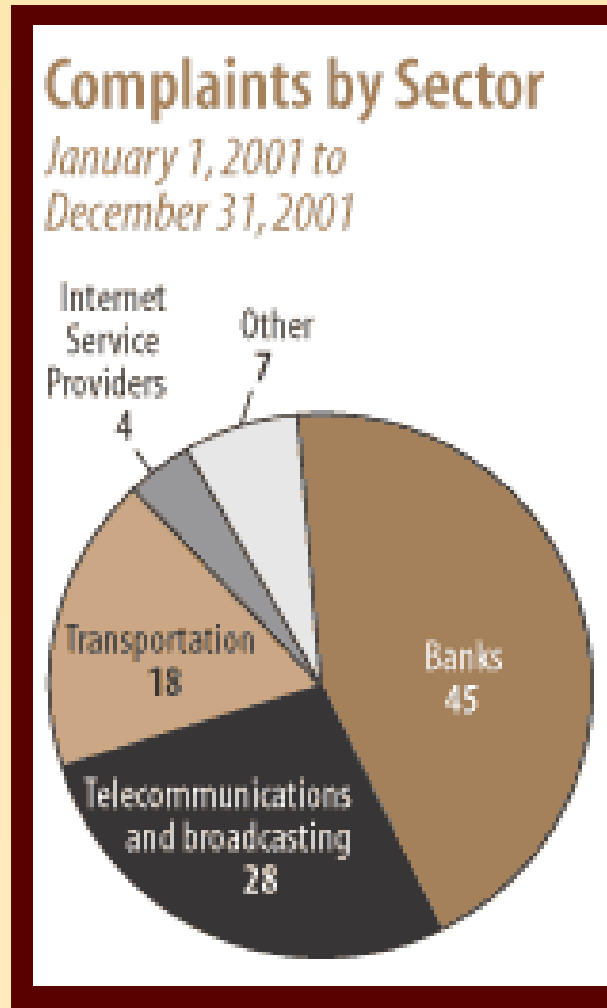
- Commissioner may issue report following investigation:
 - Findings/recommendations
 - No binding orders

- Court remedies are available:
 - Order organization to correct practices
 - Award damages (includes humiliation)



Complaints by Sector under *PIPEDA*

**January 1, 2001 to
December 31, 2001**





Implications for Data Systems

- Consent must be the basis for systems development:
 - Is express consent required?
 - Is notice clear and unambiguous?
 - Has privacy policy been developed and posted?
 - Is proposed use/disclosure reasonable?



Privacy by Design

- Need to build in privacy requirements from the start: Build it in!
 - How is consent being captured/recorded?
 - Do access controls reflect consent?
 - Is security adequate –against both internal and external threats?
 - Does system provide for access to data and correction by the data subject?
 - Is there a robust audit function and audit trails?



Security legislation - Implications

- Security legislation may impact on database design (to the detriment of privacy)
 - *Patriot Act; Aviation and Transportation Security Act; Canada's Lawful Access Initiative*

- Government desire for greater access to private databases (e.g. Computer Assisted Passenger Pre-Screening II (CAPPS II) program)



The Final Word

STEPS:

Security Technologies

Enabling Privacy

- Need both security *and* privacy: as two sides of an indivisible whole
- www.ipc.on.ca/docs/steps.pdf

How to Contact Us

Commissioner Ann Cavoukian

Information & Privacy

Commissioner/Ontario

80 Bloor Street West, Suite 1700

Toronto, Ontario M5S 2V1

Phone: (416) 326-3333

Web: www.ipc.on.ca

E-mail: commissioner@ipc.on.ca

