

PIPEDA,
What Happens if You Do Not Comply

by Alex Zivkovic

ISO 17799 User Group Conference
January 30, 2004
Toronto, Canada

Kligerman & Associates
BARRISTERS & SOLICITORS

PIPEDA (Canada)

- In 2001 applied to the federally regulated private sector
 - airlines; banking; broadcasting; telecommunications
- In 2002 applied to every organization that deals with personal health information
- In 2004 applied to every organization that collects, uses or discloses personal information in the course of commercial activity.
 - Except where similar provincial legislation has been enacted, in which case the provincial legislation will apply

Let's see...

Sally filed a change of address request...

John consents to gift delivery, but is
opting out of the newsletter...

Billy is challenging his "naughty" status...



Enforcement of *PIPEDA*

Kligerman & Associates
BARRISTERS & SOLICITORS

Where Does One go With a Complaint?

- Privacy Commissioner of Canada
 - Jennifer Stoddart
 - any federal government agency, department, ministry
 - any organization that collects personal data
- Information & Privacy Commissioner of Ontario
 - Ann Cavoukian (since 1997)
 - any Ontario government body
 - any local government body

PIPEDA - Complaint Procedure

1. Complainant:
 - contacts organization directly
 - contacts organization's industry association
2. Contact Privacy Commissioner's Office to lodge a complaint (free & no need for a special advisor)
3. Commissioner decides whether to "initiate" the complaint

PIPEDA - Complaint Procedure (cont)

4. Commissioner gives notice of the complaint to the organization
5. Commissioner investigates the complaint
 - questions persons and reviews documents
 - enters any premises
6. Commissioner prepares a report within one year after complaint was filed
 - states findings (well-founded; not well-founded)
 - gives recommendations on how to fix the non-compliance

PIPEDA - Complaint Procedure (cont)

7. Complainant may apply to Federal Court for a hearing within 45 days of the report
8. Court may:
 - order organization to correct practices
 - award damages to the complainant

Meanwhile in Ontario

- Federal government is really hoping the provinces will pass their own privacy laws
- Constitutional challenge possible
 - trade and commerce
 - vs
 - property and civil rights

PPIA

Ontario Attempts to Pass Privacy Legislation

- A draft *Privacy of Personal Information Act* (Ontario) was put forth in February 2002
- 600 submissions later...
- The Eaves government did not introduce the bill
- Only bill remaining is *Health Information Protection Act*, 2003 - Bill 31 in the current legislature

Not the law

Commissioner's Powers under *PPIA*

Very strict enforcement provisions and powers:

- Commissioner has power to:
 - review subject-matter of complaint
 - inspect and investigate
 - order organization to comply (not the case with *PIPEDA*)
- Divisional Court has power to:
 - vary or set aside Commissioner's order
- Superior Court of Justice has power to:
 - award damages

Not the law

Damages Under *PPIA*

Factors for the court to consider:

- non-compliance intentional or inadvertent
- actual harm suffered
- any mitigation done
- economic loss/loss of income
- any humiliation or psychological damage
- duration of the harm suffered

Not the law

Offences Under *PPIA*

Offence to:

- collect personal information by way of deception or coercion
- obtain access to personal information in bad faith
- dispose of personal information to evade request for access
- obstruct Commissioner's doings
- knowingly deceive Commissioner
- fail to comply with Commissioner's order

Not the law

Offences Under *PPIA* (cont)

Defence:

- due diligence or acting as a reasonably prudent person would in the circumstances

Penalty if convicted of the offence:

- max fine of \$50,000 for an individual
- max fine of \$250,000 for a company

Not the law

Some Complaints Under the *PIPEDA*

Kligerman & Associates
BARRISTERS & SOLICITORS

Prescription Writing Profiles

- Dr. Albert Shumacher
- IMS Health Canada
- Complaints #14 and #15 in front of PCC
- Enter Ronald Maheu
- Application for judicial review of Commissioner's finding to the Federal Court Trial Division
- Federal Court of Appeal

Bank Conducts Credit Checks Without Consent

- Bank conducted credit cheques on its existing customers
- To determine their eligibility for overdraft protection
- If customers accepted the new service they were asked to sign authorization for the already performed credit cheque

Use of Electronic Signatures

- Improper collection of personal information by demanding electronic signature upon delivery of parcels
- Posting of signatures on the company website without consent
- Potential for subsequent non-consensual use and disclosure of his electronic signature by the company.

Asking for SIN

- Bank can ask for SIN# for opening new account (has obligations to report interest income to CCRA)
- Telephone company can ask for SIN# because reasonably appropriate that telco needs to find out about creditworthiness of customer
- Applicants for a loan with the bank cannot be required to reveal their SIN# as condition of service

Airline Company's Use of Cookies

- Individual denied access to airline's website because his browser configured to disable cookies
- Airline company collects personal information about its website visitors:
 - country of origin, language preference (permanent)
 - name, mileage, country of origin, language (temporary)

Thank You

Kligerman & Associates
BARRISTERS & SOLICITORS