

# **NUTS AND BOLTS OF PRIVATE SECTOR PRIVACY LAW IN CANADA: WHAT YOU NEED TO KNOW**

**Interactive Screen Presentation  
Banff – July 16, 2003**

**Ravi N. Shukla  
rshukla@langmichener.ca**

Lang Michener

# The New Privacy Laws - Background and Context

- OECD Guidelines (1980)
- EU Data Protection Directive (1995)
- CSA Personal Information Protection Principles (1995)
- Quebec Privacy Act (1993)
- PIPEDA (2000)

# PIPEDA - Compliance Framework

- Comprehensive regime to address the protection of personal information collected, used, maintained and disclosed for commercial purposes
- Addresses not only procedures and documents but also the infrastructure required
- Policies and procedures must also address responsibility, security, access to information and dispute resolution

# PIPEDA - Transition to Effectiveness

- Jan 1, 2001 - all federally-regulated commercial organizations and cross-border transfers of personal information except re: health
- Jan 1, 2002 - all of the above now including health information
- Jan 1, 2004 - all organizations in respect of their commercial activities unless otherwise governed by substantively similar provincial legislation - however cross-border transfers of information continue to be subject to PIPEDA

# PIPEDA - Transitional Issues

- No grandfathering - need to make databases compliant today if want to use them in 2004 and beyond
- What are compliance requirements?
  - ◆ consent
    - opt-in/opt-out
    - implied or express
    - by minors
  - ◆ disclosure of purposes
  - ◆ procedures for business transactions, employees, health information

# PIPEDA - Transitional Issues (cont'd)

- Guidance from Privacy Commissioner
- Articulation of provincial rules
- Why organizations need to know:
  - ◆ to ensure that current procedures comply - to qualify information
  - ◆ to avoid costly procedural changes in the future

# PIPEDA - Major Areas of Impact

- Delivery of products - e.g. financial services, telecommunications, credit cards, health services
- Customer Relationship Management
- Customer service/warranty
- Customer contact
- Billing and internal administration
- Future marketing
- Employee privacy

# What is Personal Information?

- Information about an identifiable individual (very broad)
- Compare detailed statutory definitions (Privacy Act, Credit Reporting Acts)
- Recorded and unrecorded
- Does not include “work product” (IMS Health case)
- Issues: professional opinions; credit scores
- Significant e-commerce impact: (privacy policies, spam)

# Compliance Requirements - Procedures for Database Users

- Disclosure Notice - statement of purposes (what information, what uses, to whom disclosed)
- However only purposes that are reasonable in the circumstances
- Obtain consent to stated purposes
- Opt-in (express) consent is preferable and required for sensitive information (e.g. financial)
- Opt-out (implied) consent may be used for non-sensitive information (e.g. contact)
- Must make opt-out procedure accessible, no cost

# Compliance Requirements - Organizations

- Develop corporate privacy procedures and policies
- Establish compliance framework including procedure manual/system
- Corporate privacy office
- Activate audit/review/adjustment procedures

# Developing Corporate Privacy Policies

Why:

- mandated by PIPEDA
- effective means to achieve and maintain compliance (internally)

What:

- operating policies and procedures
- corporate privacy code
- consumer brochure

How:

- formulate plan of work
- check-lists
- execute

# Privacy Policies - Statutory Framework

- PIPEDA requires compliance with CSA Model Code
- Code Principles
  - Accountability
  - Limiting Use, Disclosure, Retention
  - Openness
  - Challenging Compliance
- PIPEDA, s.24 Privacy Commissioner's mandate to encourage development

# CSA Model Code

## ➤ Principle 1 - Accountability

- ◆ Organizations shall implement policies and practices to give effect to these principles, including:
  - (a) procedures to protect personal information
  - (b) procedures for complaints and inquiries
  - (c) training and communicating to staff about the organization's policies and practices
  - (d) developing materials to explain their policies and procedures

# CSA Model Code

## ➤ Principle 2 – Identifying Purposes

- ◆ The purposes for which personal information are collected shall be identified by the organization at or before the time the information is collected.

# CSA Model Code

## ➤ Principle 3 – Consent

- ◆ The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

# CSA Model Code

## ➤ Principle 4 – Limiting collection

- ◆ The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

# CSA Model Code

- Principle 5 - Limiting Use, Disclosure and Retention
  - ◆ Organizations shall develop guidelines and implement procedures respecting the retention and destruction of information, including minimum and maximum retention periods

# CSA Model Code

## ➤ Principle 6 – Accuracy

- ◆ Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

# CSA Model Code

## ➤ Principle 7 – Safeguards

- ◆ Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

# CSA Model Code

## ➤ Principle 8 - Openness

- ◆ an organization shall make readily available information, and shall be open about its policies and practices
- ◆ individuals shall be able to acquire information about the policies and practices without unreasonable effort - in a form that is generally understandable
- ◆ may make information available in a variety of ways (e.g. brochure, 1-800 no., web site)

# CSA Model Code

- Principle 9 - Challenging Compliance
  - ◆ organizations shall put procedures in place to receive and respond to complaints or inquiries;
  - ◆ procedures should be easily accessible and simple to use.

# CSA Model Code

- Principle 10 – Challenging compliance.
  - ◆ An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

# Objectives of Privacy Policies/Procedures

- Internal operating policies and procedures - detailed compliance with PIPEDA, based on activity-specific requirements
- Corporate privacy code - provides principles that guide organization's compliance and serve as benchmarks
- Together they enable organizations to meet due diligence obligations (on-going monitoring/auditing/adjustment)
- Consumer brochure - satisfies communication and openness requirements

# Privacy Implementation - Summary

- Must activate now to be compliant in 2004 - no grandfathering
- Requires compliance infrastructure including policies, procedures, documents
- Organizations need guidance to address grey areas
- Best approach:
  - ◆ methodical development
  - ◆ privacy infrastructure
  - ◆ compliance reference system
  - ◆ audit and monitoring