Privacy Legislation

Lunch and Learn Session
Roger Guy Baguley
March

PIPEDA: An Overview

- PIPEDA: *Personal Information Protection and Electronic Documents Act*
- Addresses the collection, use, and disclosure of personal information
- Application staggered over three years

Privacy Legislation: Prior to January 1, 2004

PIPEDA Application

- Federal works, undertakings, or businesses:
  - personal information that is collected, used, or disclosed in the course of commercial activities; and
  - personal information that is collected, used, or disclosed of an employee of a federal work, undertaking, or business

- Non-“federal works, undertakings, or businesses:” personal information that is disclosed across provincial or national borders for consideration (e.g. companies who sell their customer information across borders)

Privacy Legislation : After January 1, 2004

PIPEDA Application

- Personal information that is collected, used, or disclosed in the course of commercial activities within a province
- Exception: due to constitutional issues, PIPEDA will not apply to employees' personal information collected, used, or disclosed by provincially regulated employers
- Prudent for employers to consider their practices regarding personal information of employees now given likelihood of provincial legislation

Privacy Legislation : After January 1, 2004

- The federal government may exempt organizations and/or activities in provinces that have adopted “substantially similar” legislation
- “Substantially similar” means equal to or superior to PIPEDA
- Quebec: *Act respecting the protection of personal information in the private sector* (in force 1994)
- British Columbia: *Personal Information Protection Act* (in force 2004)
- Alberta: *Personal Information Protection Act* (tabled May 2003)
- Ontario: *Privacy of Personal Information Act, 2002* (draft)

Privacy Legislation : After January 1, 2004

- When a province has “substantially similar” legislation, PIPEDA will apply to:
  - personal information that flows across provincial or national borders; and
  - any organizations or activities which are not covered by the “substantially similar” provincial legislation

PIPEDA: Exemptions to Application

- PIPEDA does not apply to:
  - any government institution subject to the *Privacy Act*;
  - personal information collected, used, or disclosed by an individual for personal or domestic purposes (e.g. an individual's Christmas card list); and
  - personal information collected, used, or disclosed by an organization for journalistic, artistic, or literary purposes

PIPEDA: Purpose

A Balancing Act

Section 3:

The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use, and disclosure of personal information in a manner that recognizes the **right of privacy of individuals** with respect to their personal information and the **need of organizations** to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances

PIPEDA: Key Definitions

Personal Information

Information about an identifiable individual, but does not include the name, title, or business address, or telephone number of an employee of an organization

Examples:

- age, weight, height, marital status, religion, race, ethnic origin, income, medical records, etc.

PIPEDA: Key Definitions

Commercial Activity

Any particular transaction, act, or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering, or leasing of donor, membership, or other fundraising lists

PIPEDA: Privacy Principles

Principle 1: Accountability

Responsibilities

- Comply with all of the privacy principles
- Appoint an individual or individuals to be responsible for ensuring compliance
- Protect all personal information held by your organization or transferred to a third party
- Develop and implement personal information policies and practices

PIPEDA: Privacy Principles

Principle 1: Accountability

Actions

- Ensure that your privacy officer is accessible to internal and external inquiries
- Analyze all personal information handling practices
- Develop and implement policies and procedures to protect personal information
- Inform and train employees on privacy policies and procedures
- Include a privacy protection clause in your contracts to:
  - guarantee that third parties provide the same level of protection as your organization; and
  - protect the personal information from sub-contracting by third parties

PIPEDA: Privacy Principles

Principle 1: Accountability

When transferring personal information to third parties:

- limit the use of the personal information to the purposes specified by your contract;
- limit disclosure of the personal information to what is authorized by your organization or required by law; and
- use appropriate security measures to protect the personal information

PIPEDA: Privacy Principles

Principle 2: Identifying Purposes

An organization may collect, use, or disclose personal information **only** for purposes that a **reasonable person** would consider are **appropriate** in the circumstances

PIPEDA: Privacy Principles

Principle 2: Identifying Purposes

Responsibilities

- Before or when personal information is collected, identify and document why it is needed and how it will be used
- Inform the individual from whom the personal information is collected why it is needed
- Identify any new purpose for the personal information and obtain the individual's consent before using it

PIPEDA: Privacy Principles

Principle 2: Identifying Purposes

Actions

- Review your personal information holdings and ensure that they are all required for a specific purpose
- Ensure that purposes are limited to what a reasonable person would expect under the circumstances
- Record all identified purposes and obtained consents

PIPEDA: Privacy Principles

Principle 3: Consent

Responsibilities

- Inform the individual, in a meaningful way, of the purposes for the collection, use, or disclosure of personal information
- Obtain the individual's consent before or at the time of collection and when a new use is identified
- Consent cannot be obtained by deceptive means
- If an individual withdraws consent, must inform the individual of the resulting implications

PIPEDA: Privacy Principles

Principle 3: Consent

- The form of consent (i.e. express or implied based on conduct) may vary, depending on the **circumstances,** the **type of personal information**, and the **reasonable expectations** of the individual
- An organization should seek express consent with sensitive personal information
- Cannot be made a condition for supply, unless the personal information requested is required to fulfill an explicitly stated and legitimate purpose
- Exceptions to obtaining consent only in specific circumstances

PIPEDA: Privacy Principles

Principle 3: Consent

- In order to continue to use or disclose personal information that was collected prior to the application of PIPEDA, consent must be obtained
- If new purpose, then new consent must be obtained
- In order for consent to be enforceable, the collection, use, or disclosure must be reasonable

PIPEDA: Privacy Principles

Principle 3: Consent

Actions

- Ensure individuals understand how their personal information will be used before obtaining consent
- Record consent obtained

PIPEDA: Privacy Principles

Principle 4: Limiting Collection

Responsibilities

- Limit the amount and the type of personal information collected to what is necessary to fulfill the identified purpose

PIPEDA: Privacy Principles

Principle 5: Limiting Use, Disclosure, and Retention

Responsibilities

- Use or disclose personal information only for the purpose for which it was collected, unless the individual consents or the use or disclosure is authorized by law
- Retain personal information only as long as necessary to satisfy the identified purposes
- Destroy, erase, or make anonymous personal information that is no longer required for an identified purpose or a legal requirement
- Develop guidelines and implement procedures regarding retention and destruction of personal information

PIPEDA: Privacy Principles

Principle 5: Limiting Use, Disclosure, and Retention

Actions

- Institute minimum and maximum retention periods that take into account legal requirements or restrictions and redress mechanisms
- Conduct regular reviews to determine whether personal information is still required
- Dispose of personal information in a way that prevents improper access

PIPEDA: Privacy Principles

Principle 6: Accuracy

Responsibilities

- Minimize the possibility of using incorrect personal information when making a decision about an individual or when disclosing personal information to third parties

PIPEDA: Privacy Principles

Principle 6: Accuracy

Actions

- Keep personal information as accurate, complete, and up to date as necessary, taking into account its use and the interest of the individual
- Update personal information only when necessary to fulfill the specified purpose

PIPEDA: Privacy Principles

Principle 7: Safeguards

Responsibilities

- Protect personal information from:
  - loss and theft; and
  - unauthorized access, disclosure, copying, use or modification

PIPEDA: Privacy Principles

Principle 7: Safeguards

Actions

- Develop and implement a security policy to protect personal information
- Regularly review and update security measures
- Security measures can take the form of:
  - physical (e.g. locks on doors and cabinets);
  - organizational (e.g. security clearances); and
  - technological (e.g. password protection and encryption)

PIPEDA: Privacy Principles

Principle 7: Safeguards

Actions

- The following factors should be considered when selecting appropriate safeguards:
  - sensitivity of personal information;
  - amount of the personal information;
  - extent of distribution;
  - format of the personal information; and
  - type of storage
- Ensure employees understand the importance of maintaining the security and confidentiality of personal information

PIPEDA: Privacy Principles

Principle 8: Openness

Responsibilities

- Make readily available information about policies and practices relating to the management of personal information. This information should include:
  - name or title and address of person accountable for privacy policies and practices and to whom complaints or inquiries can be forwarded;
  - how to gain access to personal information;
  - a description of the type of personal information maintained;
  - a description of the type of personal information made available to third parties; and
  - copies of brochures or other information which explain privacy policies and practices

PIPEDA: Privacy Principles

Principle 8: Openness

Actions

- Ensure employees are familiar with policies and practices relating to the management of personal information so that they can respond to individual inquiries

PIPEDA: Privacy Principles

Principle 9: Individual Access

Responsibilities

- Exceptions to access are limited
- Individuals have the right to:
  - know what personal information an organization has about them;
  - know how personal information is used and to whom it is disclosed;
  - access to their own personal information; and
  - have their own personal information amended

PIPEDA: Privacy Principles

Principle 9: Individual Access

Actions

- Organizations must respond to an access request no later than 30 days after receipt of the request (exceptions to this time period are limited)
- Provide access at minimal or no cost to the individual
- Notify the individual of approximate costs before processing a request
- If an access request is refused, the organization must inform the individual of the reasons for its refusal, in writing, and outline any recourse the individual may have under PIPEDA

PIPEDA: Privacy Principles

Principle 10: Challenging Compliance

Responsibilities

- Develop and implement simple and easily accessible procedures to receive and respond to complaints or inquiries
- Investigate all complaints received
- Take appropriate measures to amend personal information handling policies and practices, if necessary

PIPEDA: Privacy Principles

Principle 10: Challenging Compliance

Actions

- Promptly acknowledge receipt of a complaint
- Assign the investigation of a complaint to an individual with the necessary skills and who will conduct the investigation in a fair and impartial manner
- Promptly notify individuals of the outcome of a complaint
- Correct any inaccurate personal information
- Assess policies and practices against complaints

Role of the Privacy Commissioner

- Has oversight over PIPEDA
- Accepts and investigates complaints from individuals alleging a contravention of PIPEDA
- Can also initiate a complaint against an organization
- Mediation and conciliation may be used to settle matters between complainant and organization
- Must report findings of investigation

Role of the Privacy Commissioner

- Penalties under PIPEDA:
  - an offence punishable on summary conviction and liable to a fine not exceeding $10,000.00; or
  - an indictable offence and liable to a fine not exceeding $100,000.00
- As of April of 2003, no penalties have been issued

Role of the Privacy Commissioner

- Under certain circumstances, an application can be made to the Federal Court, Trial Division
- The Court may:
  - order an organization to correct its practices in order to comply with PIPEDA;
  - order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not the Court ordered such correction; and
  - award damages to a complainant, including damages for any humiliation that the complainant has suffered

Role of the Privacy Commissioner

- May also audit the personal information practices of an organization if he has reasonable grounds to believe that the organization is contravening a provision of PIPEDA or is not following a recommendation in Schedule 1
- Must report findings of the audit and provide the organization with any recommendations considered appropriate
- May also make public any information relating to the personal information practices of an organization if it is in the public interest to do so

Considerations for Panigas in Commercial Context

Consider the collection of personal information in the following circumstances:

- the opening of a new office, site &/or shop;
- contests/promotions;
- customer preference programs;
- marketing; and
- customer contact

Considerations for SHRS as an Employer

- Identify specific purpose for collection, use, or disclosure of personal information
- Obtain employee's consent
- Safeguarding personal information
- Retention and destruction policies and practices
- Disclosure of personal information to third parties (including related companies and subsidiaries)
- Example: use of Social Insurance Number

Next Steps

- Conduct an information audit
- Appoint a Privacy Officer
- Develop process for who are responsible for ensuring compliance
- Develop policies and practices addressing management, retention, and destruction of personal information
- Continue to assess policies and practices over time; modify if necessary