Privacy

A Practical Overview

Victoria Prince

Lisa Katz Jones

Borden Ladner Gervais LLP

February 25, 2004

Lawyers

Patent and Trade-mark Agents

PRIVACY BASICS

Personal Information: Information about an identifiable individual in any format, on any medium

Think of it as the individual's personal property (for example, a car). You can use it, but only if you get permission first!

Not employee name, title, business address and phone number

Applies to: As of January 1, 2001 to federal undertakings and as of January 2, 2004, to:

every organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activities

PRIVACY BASICS

Application of PIPEDA:

- Subject to provincial privacy legislation where it exists
  - Ontario – no
  - Quebec – yes
  - Alberta – yes
  - British Columbia – yes
  - All other provinces – no
  - Northwest Territories/Yukon/Nunavut – Federal legislation applies

Employees

- The general assumption is that PIPEDA only deals with information relating to employees for federal undertakings
    - although some experts believe that a strong argument can be made to the effect that PIPEDA applies to the information of unionized employees, and that the Federal Privacy Commissioner would be sympathetic to an argument that PIPEDA applies to all employee relationships.
- Provincial privacy legislation does apply to employee information
- Need to consider where carry on business to ascertain what law applies,
- Best practices to have procedures in place to ensure compliance with PIPEDA vis-à-vis your employees, regardless of where you carry out your business.

PRIVACY BASICS

NO GRANDPARENTING

There is no general exception for information collected before PIPEDA came in force:

- you do not have to go back and get consent for having collected it in the first place

BUT

- you will need consent to use or disclose now

PRIVACY BASICS

Ten Principles

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

REMEMBER PURPOSE, SENSITIVITY OF INFORMATION, CONSENT

1. Accountability Requirements

"An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable."

The identity of the individual shall be made known upon request.

Accountability extends to all information in an organization's "possession or custody", including information that has been transferred to a third party for processing.

Contracts with third parties should ensure a "comparable level of protection".

You must have policies and procedures that give effect to the principles and regularly update and monitor.

1. Accountability Actions

Appoint a Chief Privacy Officer or Committee ("CPO") and:

- Agree on the CPO's List of Duties
- Make sure everyone knows who the CPO is
- Be ready to tell people who the CPO is

Accountability Actions

CPO should take the lead to:

- Implement procedures to protect personal information
- Implement procedures to receive and respond to complaints and inquiries
- Train staff
- Communicate to staff about the policies and procedures
- Develop information to explain the policies and procedures
- Review third party relationships and use contracts to ensure comparable protection

2. Identifying Purposes--Requirements

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

Identifying the Purpose is a key step in getting consent:

"*The purpose of stating a purpose is to present an individual with a proposition for consideration whether to accept or reject." (Privacy Commissioner's Finding, Number 176)*

• Consent Requirements

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

Note: PIPEDA specifies exceptions, which define entirely what is "appropriate"

3. Consent Requirements

Knowledgeable Consent:

- **PIPEDA requires "knowledge and consent"**
- **You must make a reasonable effort to ensure that the person is "advised" of the purposes for which the information will be used**
- **Purposes must be stated in such a manner that the person can reasonably understand how the information will be used or disclosed**

3. Consent Requirements

Forms of Consent

- **Implied, e.g., subscription renewal, pizza delivery**
- **Negative option or "opt-out": e.g., "check the box" if you do not consent**
- **Express: written (or click-through) or oral (but then how to prove it?)**

3. Consent Requirements

What form do you need?

Depends on:

- **Sensitivity**
- **Reasonable expectations**

4. Limiting Collection Requirement

"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."

- **Reasonableness, not just consent**
- **<u>Necessary</u> to fulfill purpose identified**

4. Limiting Collection Actions

Don't Extort

Do not, as a condition of supplying a product or service, *require* a person to consent to the collection, use, or disclosure of information beyond that required to fulfill the *explicitly specified* and *legitimate* purposes.

Examples: birth date, SIN, signature

5. Limiting Use, Disclosure and Retention

"Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of these purposes."

- **New purpose = new consent**
- **Routine file destruction policy-but be careful about employee information and potentially litigious information**
- **Obligation to keep information for Access Requests**

Disclose vs. Transfer

- Disclosing personal information requires CONSENT
- Transferring does not—but make sure that the party getting the information complies with PIPEDA
- Contractual matter

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."

- **Update BUT**
- **Do not keep or update if not "necessary" for the purpose**
- **Comply with Access rules**

7. Safeguards

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

- **Avoid:**
  - **Loss, theft**
  - **Unauthorized access, disclosure, copying, use or modification**
- **Have policies, procedures and technology to address:**
  - **Physical access**
  - **Electronic access**
  - **Staff awareness**
  - **Destruction/disposal procedures**
- **Plan to deal with security breaches**

8. Openness

"An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."

- **Have a policy!**
- **Make it easy to get**
- **Make it clear and make sure it tells people:**
  - **Type of information you hold**
  - **Generally how you use it**
  - **What you disclose to related organizations/others**
  - **Name/title/address/contact for "accountable person"**
  - **How to get access**
- **Train staff, especially if they deal with the public**

9. Individual Access

"Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."

- **Must have method for allowing access to individual's information**
- **Respond within "reasonable time" = no more than 30 days**
- **Must correct errors identified by individual**
- **Investigate <u>all</u> complaints**
- **Be prepared to do something if complaint is justified**

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."

- **Not restricted to persons whose information you hold**
- **Process for complaints**
- **CPO's job to respond**
- **Be ready to change policies and practices in response**

Industry-Specific Questions

- Q. Should pharma companies assist in managing the relationship between sales reps and physicians?
- A. To the extent that personal information about physicians is collected, used and disclosed to or by **sales reps**, the responsibility for compliance with PIPEDA rests with the sales rep. If the **pharma company** itself collects, uses or discloses the personal information of physicians, the **pharma company** will be responsible for compliance with PIPEDA. Ultimately, though, best business practices would suggest, that in any pharma companies should be satisfied that the collection, use and disclosure of the relevant personal information.

Industry Specific Questions

- Q. How does PIPEDA impact information that is mandated to be collected by Health Canada regulations (e.g. AE reporting, complaint handling, consent from clinical trials)?
- A. PIPEDA does not have an express exemption from the requirement to obtain consent to the collection and use of personal information even where such collection and use is required by law. However, it is unlikely that the current privacy commissioner will determine that collection and use of personal information as prescribed by law is not permitted under PIPEDA, **but** the jury is still out.

Industry-Specific Questions

- Q. What about discussions with health professionals and Key Opinion Leaders (KOLs) that are used by the marketing arms of pharma companies when they are devising marketing and sales strategies?
- A. To the extent that these discussions result in the KOLs divulging their personal preferences, opinions etc. or to the extent that personal information gleaned from these discussions is otherwise collected, used or disclosed, it is necessary to comply with PIPEDA.

What should you do?

- Know what "information" you collect, how you use it, and whom you disclose it to
- Have a privacy policy
- Train your employees about privacy matters
- Think about a website policy
- Appoint a CPO
- GET CONSENT(S)!
- Be accurate and careful with information
- **Stay out of trouble:** *ASK YOUR LAWYER!*

Thank You

Victoria Prince

Lisa Katz Jones

vprince@blgcanada.com

Lkatzjones@blgcanada.com

Borden Ladner Gervais LLP

February 25, 2004

BORDEN
LADNER
GERVAIS

Lawyers

Patent and Trade-mark Agents

INTELLECTUAL PROPERTY
SCOTT & AYLEN
PROPRIÉTÉ INTELLECTUELLE