

Brooks Newsletter

January 2004

THE PRIVACY ACT: IS ITS BARK WORSE THAN ITS BITE?

The Federal government's privacy act, the *Personal Information Protection and Electronic Documents Act* (or **PIPEDA** for short), has received much attention recently. However, many business people remain wondering: what is PIPEDA and what does it mean for my business?

1. What is PIPEDA?

PIPEDA aims to protect an individual's personal information from improper disclosure and use by requiring organizations to comply with the act's safeguards, which includes obtaining consent for the use of personal information, developing privacy policies for the handling of such information and appointing a privacy officer. (**Note:** In provinces where legislation "substantially similar" to PIPEDA has been enacted, businesses would comply with that province's legislation. Ontario has not passed comparable legislation so Ontario businesses must comply with PIPEDA.)

2. Does it apply to my organization?

The answer to this question is likely now yes. PIPEDA originally applied only to the commercial activities of federally-regulated undertakings and business, but its scope has been recently expanded. As of January 1, 2004, PIPEDA applies to every Canadian organization that collects, uses or discloses personal information in the course of commercial activity within a province. Unfortunately, there are no minimum size requirements for application. As the Federal Privacy Commissioner (the Commissioner) recently said, "It's going to hit all kinds and sizes of businesses in Canada."

There are however a number of exemptions about which businesses should be aware. First, to be caught by the act's apparatus the activity in question must be of a "commercial character". Second, PIPEDA does not apply to personal information collected, used or disclosed for journalistic, artistic or literary purposes. Third, while employee information is not currently protected, it would wise to treat it no different from other personal information since it is likely that new provincial legislation will soon address employee information. As well, Section 7 outlines situations in which legal and social purposes overrule the need to obtain consent, such as: when required by law, involving debt collection and protecting one's life or safety.

At the end of the day however, most Canadian businesses, no matter how big or small, must comply with PIPEDA.

It is important to note that PIPEDA does not allow for the "grandfathering" of pre-existing information. This means that companies must implement measures to deal with not only personal information received in the future but also that which the company already possesses, including obtaining after-the-fact consent.

Visit the Federal Privacy Commissioner's Web site at www.privcom.gc.ca for compliance tips. Also, go to www.pipeda.org and www.privacyinfo.ca for more information on this topic.

3. What is personal information?

PIPEDA deliberately defines "personal information" broadly as "information about an identifiable individual." According to the Commissioner's Guidelines, the definition

Brooks Newsletter

January 2004

encompasses such information as name, age, weight, height, medical records, income, purchases, spending habits, race, ethnic origin, colour, blood type, DNA code, fingerprints, marital status, religion, education, home address and telephone number.

While the definition of personal information notably excludes the name, title or business address or telephone number of an employee of an organization, as alluded to above, it would be wise to treat employee information with the same care as other personal information.

4. What does it mean for my company?

We outline below what businesses must do when they collect, store and use or disclose personal information, based on the 10 key principles outlined in PIPEDA:

- i. **Accountability:** Appoint an individual to be responsible for your organization's compliance (a.k.a. a Privacy Officer); ensure any information transferred to third party is adequately protected.
- ii. **Identifying purposes:** Identify the reasons and purposes (which must be reasonable in the circumstances) for collecting personal information before or at the time of collection.
- iii. **Consent:** Inform and obtain the individual's consent before or at the time of collection, as well as when a new use is identified; depending on the sensitivity of personal information, consent can be implied from the circumstances.
- iv. **Limiting collection:** Only collect personal information that is necessary; do not deceive or mislead individuals about the reasons for collecting personal information.
- v. **Limiting use, disclosure, and retention:** 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 the act; keep personal information only as long as necessary to satisfy the purposes and then properly destroy.
- vi. **Accuracy:** Keep information as accurate, complete and up-to-date as is necessary for the purposes for which it is being used.
- vii. **Safeguards:** Protect personal information (no matter in what form stored) against loss or theft, from unauthorized access, disclosure, copying, use or modification.
- viii. **Openness:** Create and inform clients and employees of your policies and practices for the management of personal information (a.k.a. a Privacy Code), and make these policies and practices available.
- ix. **Individual access:** Upon request, inform individuals of the existence, use and disclosure of his personal information, and give them access to their information; if requested, correct or amend any personal information.
- x. **Provide recourse:** Give individuals the ability to challenge compliance with the above principles. Investigate all complaints received and take appropriate measures to correct information handling practices/policies.

Brooks Newsletter

January 2004

5. Recommendation

In order to comply with PIPEDA and the above principles, we recommend the following:

- (a) **appoint an appropriate person to be the Privacy Officer** (to oversee implementation, ongoing compliance and addressing inquiries/complaints);
- (b) analyze all personal information handling practices & address in your Privacy Code (i.e., **conduct a Privacy Audit**—simply do a chart that: identifies the kind of information being collected, used and disclosed; identifies how and for what purpose it is being used; how consent is obtained; to whom it is being disclosed; how it is safeguarded; and how and for how long it is being stored);
- (c) **obtain necessary and appropriately-worded consents** from clients, customers and suppliers for both past and future collection, use and disclosure (review documentation such as engagement letters to ensure you obtain appropriate consents in such documents);
- (d) **develop and make available policies/practices** with the principles in Section 4 of this article in mind (a.k.a. a Privacy Code) and produce internal policies/practices for company employees;
- (e) **train your staff** in the act's requirements/principles and your internal policies;
- (f) **be prepared for access requests** and complaints/inquiries about practices; and
- (g) **keep all personal information current.**

6. What happens if we don't comply?

Unless a complaint is lodged against your business, little will likely happen. Though the Privacy Commissioner cannot penalize for non-compliance or force businesses to implement its measures, companies that do not abide by the act's requirements take risks.

The Commissioner's mandate is to investigate complaints received about a business' privacy practices. To this end, the Commissioner has been given broad powers to investigate, mediate and conciliate complaints. If appropriate, the Commissioner would produce a report requesting particular remedial measures. Mostly though, the Commissioner negotiates and works with businesses to remedy non-compliance. The Commissioner is also empowered to publicly reveal information concerning a business' privacy practices, or lack thereof, but has so far eschewed such a policy. The report may be taken to the Federal Court for implementation, whereupon the court may also order unlimited damages to the complainant, including punitive damages for humiliation.

There are also "offences" under PIPEDA of which businesses should be aware. It is an offence to (i) destroy personal information that has been requested; (ii) retaliate against an employee who has lodged a complaint or refuses to contravene certain sections of PIPEDA; and (iii) obstruct the Commissioner's investigation. Such offences are punishable by fines of up to \$100,000.00.

Brooks Newsletter

January 2004

7. Conclusion

At first, complying with PIPEDA may seem onerous. However, once a business' privacy house is in order, there is likely to be minimal ongoing effort required. This is not to say that the task should be taken lightly: compliance will require much organizational effort. However, it is well-known that the Commissioner's office is resource-limited, so businesses have time to comply properly and fully, and do not need to panic.

What's more, the alternative of non-compliance is not a real alternative as customers/clients will come to expect full and complete protection. The reality is that good privacy practices is good business. As Ontario's Information and Privacy Commissioner recently said: "It fosters trust, builds consumer confidence, strengthens brand

recognition, increases customer loyalty and ultimately delivers competitive advantage."

If you require some further insight into PIPEDA and what your company needs to do to comply, or regarding any other legal issue, feel free to contact Brooks Barristers & Solicitors at:

Ted Maduri

Brooks Barristers & Solicitors

P: 416.920.2300 ext.23

E: ted@brookslaw.ca

Disclaimer: The foregoing provides only an overview. Readers are cautioned against making any decisions based on this material alone. Rather, a qualified lawyer should be consulted.