Advertising & Marketing Bulletin

December 2006

MARKETERS' PRIVACY LIABILITY: REVIEW OF CANADA'S FEDERAL PRIVACY LAW

Privacy International, a London-based human rights watchdog, recently ranked Canada as the second-best national defender of privacy interests, reflecting Canada's excellent reputation for legislative protection, privacy law enforcement, and leadership in promoting privacy and democratic safeguards.[1] When Privacy International runs the survey next, it is possible that Canada may jump into first place by virtue of an upcoming review and possible toughening of the Personal Information Protection and Electronic Documents Act ("**PIPEDA**"),[2] a federal privacy law that has dramatically affected the way businesses collect, use, and disclose personal information of its stakeholders.

PIPEDA, which came into force in three stages beginning in 2001, includes a provision for a mandatory review by Parliament every five years. The Privacy Commissioner of Canada ("**OPC**") has identified several privacy issues that have surfaced since PIPEDA was initially drafted in this year's PIPEDA Review Discussion Document, "*Protecting Privacy in an Intrusive World*" (the "**PIPEDA Report**").

This bulletin will briefly highlight some of the issues raised by the OPC in the PIPEDA Report, the position of the Canadian Marketing Association ("**CMA**") on such issues and the implications for businesses.

1. Overview of CMA's Position

Generally speaking, the CMA's position is that now is not the time for major changes to federal privacy law.[3] Appearing earlier this month before the House of Commons Committee on Access to Information, Privacy and Ethics, the CMA advised the committee to restrict any changes it might consider to technical amendments for purposes of clarifying meaning and intent. The CMA's position is based on the law having only applied to most Canadian businesses since January 1, 2004 and it being in the early stages of implementation. It is also based on the view, evidenced by the OPC's earlier testimony before the committee and recognized by Privacy International, that the law appears to be working well and that the OPC's "ombudsman model" powers have worked well to promote and protect the privacy rights of Canadians.

2. Blanket Consent

PIPEDA is a consent-based statute, which generally requires consent for the collection, use and disclosure of personal information. The prevailing view might be that as long as a consent clause is worded broadly enough, this will technically and legally permit a wide range of future collections, uses and disclosures under the terms of the agreement between the customer and the organization. Some privacy advocates, however, argue that truly free and informed consent requires more than a one-time, wide-open, blanket signature on a consent form.

The CMA takes the position that there is no need to amend PIPEDA to deal with the question of blanket consent given that the current provisions of the law require a degree of transparency designed to ensure that organizations are obtaining freely given, informed consent.

TAKEAWAY: Marketers should be careful when obtaining consents from their customers or employees in drafting consent forms in order to ensure that such consents are not too general in nature.

---

[1] http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269

[2] PIPEDA applies to all Canadian provinces unless a province has enacted a privacy law which has been found to be substantially similar to PIPEDA in which case the provincial law will regulate privacy matters for intra-provincial matters. As of now, only British Columbia, Alberta and Québec have enacted such privacy laws.

[3] CMA Member Bulletin No. 218, December 7, 2006.

>>>

3. Disclosure of Personal Information before Transfer of Businesses

PIPEDA contains no provision to allow an organization to disclose personal information to prospective purchasers or business partners without the consent of the individual(s) affected. Third parties may need to review this personal information (such as client lists) for their "due diligence" evaluation of whether to proceed with a transaction, such as the acquisition or sale of a business. Certain provinces have enacted privacy laws that allow disclosures without the individual's consent, subject to the execution of stringent confidentiality agreements.[4] Some may argue that it is appropriate to include a similar provision in *PIPEDA* as this would facilitate commercial transactions while others may argue that individuals should have the opportunity to opt out of the transfer of their personal information if a sale or merger occurs.

The CMA's position on this issue is that PIPEDA should allow an organization in possession of personal information to disclose that information to a prospective buyer or partner as long as contractual provisions are in place to ensure that a prospective buyer/partner will restrict their use of the information to the specified purposes and abide by other PIPEDA requirements such as safe storage and destruction of the information.

TAKEAWAY: Until PIPEDA is amended on this issue, businesses should be careful prior to disclosing personal information of their employees or clients to a potential purchaser without their employees or clients' prior consents and consider redacting personal information that is not a material consideration to the potential purchaser when fulfilling its due diligence request.

4. Breach Notification

Identity theft can occur electronically on a massive scale if organizations fail to provide adequate security for personal information. Some privacy advocates take the position that organizations that suffer security breaches or other involuntary disclosures should be required to mitigate the risk of identity theft to the individuals involved by notifying the individuals whose information is at stake, credit agencies and relevant government agencies or banks, as it may force those organizations to take security more seriously in order to avoid their security failings becoming public knowledge. On the other hand, critics of "notice" laws may argue that it is unduly expensive for organizations to carry out notifications and that consumers will start to ignore the notices, particularly if notices are required after any breach.

Prior to considering amendments to PIPEDA on this issue, the CMA suggests that the OPC consult stakeholders on this issue in order to develop and publicize national "Privacy Breach Response & Notification Guidelines" that companies should follow in cases of loss/theft of personal information.

TAKEAWAY: Organizations should report the loss or theft of information in accordance with guidelines that are geared to the sensitivity of the information and the reasonable expectations that individuals might suffer material harm as a result of the breach.

5. Transborder Flows of Personal Information

Outsourcing may involve transferring personal information outside Canada, a process described as the transborder flow of personal information. *PIPEDA* contains an accountability principle that imposes responsibility on an organization for information that has been transferred to a third party for processing by requiring the organization to use contractual or other means to provide a comparable level of protection while the information is being processed by a third party, whether this third party is in Canada or abroad.

The concern about loss of control over personal information of Canadians when it crosses borders has led to discussion about several possible options to enhance respect for this accountability principle. The CMA takes the position that there is no need to amend the law on this aspect as it feels that the accountability principle as it now stands is very strong.

[4] See privacy laws from British Columbia and Alberta.

TAKEAWAY: With the exception of releasing information as required by the laws of another country, a provision that also applies here in Canada, organizations operating in Canada have an ongoing duty to treat personal information in accordance with PIPEDA – even where that information may cross borders for processing or other reasons.

Conclusions

Regardless of any potential amendments which may be made to PIPEDA in the near future, businesses should, in order to avoid privacy liability under PIPEDA:

- be extremely careful when obtaining consents from individuals prior to collecting, using or disclosing their personal information or drafting consent forms in order to ensure that such consents are not too general in nature and are valid under PIPEDA;
- obtain legal advice in the event that they are involved in a transaction such as the merger, acquisition or sale of a business in order to ensure that the transfer or disclosure of personal information (whether of clients or employees) is made in accordance with the provisions of PIPEDA and that an agreement is entered into containing appropriate provisions designed to ensure that a prospective buyer will restrict its use of the information to the specified purposes and abide by other PIPEDA requirements such as safe storage and destruction of the information;
- obtain legal advice in the event that they suffer security breaches (or "involuntary disclosures" of personal information under their control) prior to deciding whether or not they should be notifying the individuals whose information is at stake, credit agencies and other entities such as relevant government agencies or banks of the security breach; and
- use contractual or other means when transferring personal information to a third party for processing in order to ensure that a comparable level of protection is provided while the information is being processed by such third party, whether this party is in Canada or abroad.

Information is both an asset and a potential source of liability and therefore requires accountable management practices. Do not wait until PIPEDA is amended before reviewing your organization's privacy policies to ensure your organization is ahead of the accountability curve.

Written by Eloise Gratton

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.

For further information please contact your McMillan Binch Mendelsohn lawyer or one of the Practice Leaders of our Advertising & Marketing Group listed below:

Practice Leaders

Sharon Groom 416.865.7152 sharon.groom@mcmbm.com
Bill Hearn 416.865.7240 bill.hearn@mcmbm.com

McMillan Binch Mendelsohn

TORONTO | TEL: 416.865.7000 | FAX: 416.865.7048
MONTRÉAL | TEL: 514.987.5000 | FAX: 514.987.1213
www.mcmbm.com