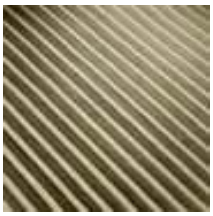
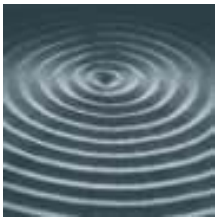


2500, 20 Queen St. West
Toronto, ON M5H 3S1
Canada
Tel. 416.595.8500
Fax.416.595.8695
www.millerthomson.com



MILLER THOMSON LLP

Barristers & Solicitors, Patent & Trade-Mark Agents

TORONTO VANCOUVER WHITEHORSE CALGARY EDMONTON WATERLOO-WELLINGTON MARKHAM MONTRÉAL

Privacy Issues in Franchise Relationships: A Practical Guide

Richard D. Leblanc

January 31, 2006

A. Introduction

On January 1, 2004, the federal government activated Part I of the *Personal Information and Protection of Personal Privacy Act* (Canada), ("PIPEDA" or the "Act")[1] to protect personal information collected, used or disclosed in the course of a commercial activity. Since that time, private businesses have been adjusting to the Canada's new privacy regime. Businesses have been required, at a minimum, to develop a comprehensive privacy policy, appoint a privacy commissioner, familiarize themselves with the elements of Canada's new private sector privacy laws, and realign their practices in order to ensure that personal information collected, used or disclosed in the course of business is handled in the appropriate manner.

Franchised businesses have not been exempt from the requirements of privacy legislation. A franchise typically requires the collection, use and disclosure of personal information at all stages of the business cycle: at the franchisee recruitment stage, at the operations level, for marketing and advertising purposes, and upon the sale of a franchised system. While privacy compliance is not without costs, the prospect of lost revenues and eroded goodwill as a result of a highly publicized privacy complaint or class action will often more than justify the expense of ensuring that appropriate privacy practices are implemented and followed. The purposes of this paper include firstly, to briefly describe the private sector personal data protection laws currently in force in Canada; secondly, to enumerate the most common privacy issues that will arise within a franchised business; and, thirdly, to provide practical suggestions and recommendations to assist franchisors and franchisees in efficiently addressing these concerns.

B. Legislation

While international legislation governing the protection of personal information has been in force for some time[2], it was not until January 1, 2001 that Canada's federal privacy legislation, PIPEDA, came into effect. At that time, Part I of the Act was activated to regulate the collection, use and disclosure of personal information by federal works, undertakings or businesses, and by certain organizations engaged in inter-provincial activities. On January 1, 2004, the remainder of the Act came into effect and has since applied to organizations which use, collect and disclose personal information in the course of their commercial activities. The Act applies in all Canadian provinces which do not have their own privacy statute. The substance of the legislation, a set of 10 guiding privacy principles borrowed from the Canadian Standards Association Model Code, is set out in Schedule I of the Act.

At the time of writing, Quebec[3], British Columbia and Alberta have adopted provincial laws which are substantially similar to the Act. The laws in British Columbia and Alberta are each called the *Personal Information and Protection Act*[4] and resulted from significant collaboration between the two provinces. Both the BC Act and the Alberta Act constitute a more complete

---

[1] S.C. 2000, c.5.

[2] The European Union adopted Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "EU Data Directive").

[3] Article 35 of the *Code Civil du Québec*, L. Q. 1991, c.64, provides that "every person has a right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person unless authorized by law." The *Loi sur la protection des renseignements personnels dans le secteur privé* (the "Quebec Act") came into effect on January 1, 1994 and was declared to be substantially similar to PIPEDA on November 19, 2003

[4] S.B.C. 2003, c.63 (the "BC Act") and S.A. Ch. P-6.5 (the "Alberta Act").

package than PIPEDA. For example, the BC and Alberta Acts each deal expressly with employee information, exclude business emails from the Acts' protection and contain exemptions for disclosures of personal information in the context of business transactions. Of notable distinction is the exemption of personal information that was collected on or before the Acts came into force. PIPEDA contains no such exclusion, underscoring the retrospective effect of PIPEDA on archived and non-current data.

Ontario does not yet have its own private-sector privacy legislation and hence PIPEDA applies in that province.

C. General Issues

1. Franchisee information

Most franchisors collect personal information from prospective franchisees during the recruitment phase. This is due to the reality that although franchisees are almost exclusively corporate vehicles which hold the licensed rights to a franchise, the franchisor ultimately views the individual principals behind the corporate licensee as the actual franchisees who uphold and perform the covenants under the franchise agreement. Accordingly, a franchisor's due diligence typically requires the disclosure of basic personal information in addition to more sensitive data such as age, marital status, banking information, salary, financial condition, employment information, credit information, driver's licence number, social insurance number, criminal records, and in some cases, health information. The franchisor's practice might be to use this information internally, to transfer it to local area developers or master franchisees, or to disclose it to third parties such as consumer reporting agencies for further analysis. Assuming a franchisee candidate is not selected to operate a franchise, the franchisor must determine what to do with the candidate's personal information, how long to retain it if it proposes to do so, and how to dispose of it.

Privacy issues also arise at the disclosure stage. Under existing Ontario and Alberta franchise legislation, the franchisor is required to provide a list of all current franchisees, as well as the name, telephone number and last known address of each franchisee that left the system in the previous fiscal year.

<u>Analysis and Recommendations:</u>

a. Recruitment: Collection from a prospective franchisee at the recruitment stage is in the interests of the individual providing the information. If this information is collected without express consent, consent to the use of the information for the purposes of assessing a candidate's suitability may be implied from the candidate's actions in completing and submitting the form for the purposes of being evaluated for suitability for the grant of a franchise. Nonetheless, given the sensitivity of much of the information, the purposes for which the information is collected should be expressly stated in the form and the explicit consent to such purposes should be obtained from each prospective candidate. The purposes for the collection of the information should include: (i) the use of the information for the purposes of assessing the candidate's suitability as a franchisee or guarantor of a franchisee; (ii) the transfer of certain of the information to a third party, such as an accountant or consumer reporting agency to conduct further due diligence; (iii) the transfer of the information to a master franchisee or area developer for assessment; (iv) the use of the information for statistical, modelling or other franchisee marketing purposes, if applicable; (v) the administration of the franchisee; (vi) the sale or transfer of the franchisor and all or any portion of its assets; (vii) disclosure to future franchisees as required by law and otherwise restricted to non-sensitive personal information;

and (viii) such other reasonable purposes as may be required from time to time. The consent should clearly relate to the purposes stated.

b. Disclosure: Under PIPEDA, the BC Act and the Alberta Act, personal information may be disclosed without consent where required by law and where the information is publicly available. "Publicly available" includes personal information in a telephone or professional or business directory.[5] As noted, Ontario and Alberta franchise legislation require the disclosure of past franchisees and their contact information and therefore, in accordance with the above-noted privacy statutes, no specific consent is required for the disclosure of prior franchisees in those provinces. In all other provinces without active franchise legislation[6], and where the information disclosed is not also contained in a professional business directory available to the public, the prior consent of the franchisee is required.

As a matter of good practice, it is advisable for franchisors to obtain consents to such disclosures, as indicated in item a. (vii) above. The franchisor's privacy policy should stipulate that such information will be retained by the franchisor only for as long as may be reasonably necessary to give effect to the purposes for which it was originally collected, or as otherwise required by law.

2. Consumer information

Consumer data is frequently collected from individual retail consumers by franchisors and franchisees for the purposes of marketing, order processing and ongoing services. Oftentimes, information is collected by the franchisee and thereafter disclosed to the franchisor, or is provided by the consumer directly to the franchisor. Information is collected from a variety of sources including through customer surveys, contests, online shopping, centralized reservations, warranty programs, affinity programs, gift cards, customer website registration and pursuant to returns policies.

This information is a treasure trove to marketers. The ease with which vast amounts of data can be manipulated in the electronic age and the resulting assault on individual privacy in the form of junk mail, spam and telemarketing has been the catalyst to the modern private sector privacy law movement. The information requested often includes the name, address, phone and email address, gender, age, income, consumer preferences, credit information, credit card information, and even digital information from the magnetic strip on debit or credit cards[7]. Prior to the advent of consumer privacy legislation, this information was often collected by distributors and franchisees and freely exchanged with manufacturers and franchisors pursuant to the terms of existing agreements. The information may have been used for primary marketing purposes and in certain cases may have been sold or rented to third parties including data brokers and commercial database operators. In addition, the information may have been transferred intra-provincially, across the border to the U.S. or another country, or may have been forwarded to a third party for warranty service, affinity program administration, order processing or some other ancillary purpose.

Analysis and Recommendations:

---

[5] See PIPEDA regulation SOR 2001-7, ss. 1 (a) and (b); B.C. Reg. 473/2003, s. 6; and Alberta Reg. 366/2003, s. 7.

[6] Prince Edward Island enacted its *Franchise Act* on June 7, 2005, but the Act will not be proclaimed into force until its regulations have been finalized.

[7] See *In re BJ's Wholesale Club, Inc.*, File No. 042-3160 (FTC).

Franchisors and franchisees must ensure at the outset that in all of their direct dealings with consumers they obtain appropriate consents for their use of personal information. As a matter of practice, the collection of non-sensitive information pursuant to an application or registration form may be construed to imply consent, especially where the purpose of the document is plainly set out, and where a franchisor's or franchisee's privacy policy is readily available and discloses the express purposes for which personal information is collected. The practice of providing consumers with the right to opt-out of receiving future communications seems to be gaining acceptance, especially in online data collection.

The collection of sensitive information, such as financial or credit card information should always be accompanied with the appropriate consent to use. In addition, principle 4.7 of PIPEDA requires that appropriate security safeguards, including the use of encryption in the case of electronically stored information, be used to by the recipient to ensure the integrity and security of the disclosed information.

All consents must be prefaced by the appropriate notice of intended purposes. The consent should state that the information will, as between the franchisor and the franchisee, become the property of the franchisor (if this is in fact the agreement between the parties), and that the consumer consents to this information being transferred to any subsequent assignee or purchaser of the franchise system.

Where personal data is being transferred extra-provincially, out of the country or to a third party service provider for any purpose including marketing, contest administration, warranty servicing, affinity program administration, or order processing, the transferor must ensure firstly that it has obtained the informed consent to such disclosures from the affected individuals. Secondly, the transferor must ensure that the privacy standards adopted by the transferee irrespective of jurisdiction are at least the equivalent of the privacy protections afforded the consumer by the transferor. The transferor must employ contractual means in order to ensure that personal information enjoys the same levels of protection in the hands of the third party as it does in the hands of the transferor.

Franchise agreements should ensure that customer lists and personal information collected by the franchisee become the property of the franchisor upon termination or expiry of the franchise agreement. Both the franchisor and the franchisee's privacy policies should provide for this anticipated disclosure as should the consent upon which the initial disclosure was based.

3. Sales of a franchise system

The now infamous Toysmart case underlined the importance of obtaining the consent to the subsequent transfer and sale of consumer data. In that case, the failed internet toy vendor Toysmart.com sought to sell its customer list which was collected online and included personal information of children. The Federal Trade Commission ("FTC") claimed that the sale constituted a deceptive act or practice contrary to section 5 of the FTC Act, in that the sale would have been in express violation of Toysmart's privacy policy. The FTC was successful in its claim and ordered Toysmart to destroy all of the personal information in issues, consisting of nearly 200,000 customers.

PIPEDA does not waive the requirements of the Act to obtain an individual's informed consent prior to disclosing his or her information to a third party in the context of the purchase and seal

of business assets. The BC Act and the Alberta Act do however permit disclosure without consent in certain business transactions, such as acquisitions, sales, leases, mergers, amalgamations or financings. In transactions to which those Acts apply, the information may be collected during the due diligence period under agreement of the recipient to use the information only for the purposes related to the business transaction, where such information is necessary for the parties to determine whether to proceed and close the transaction. The purchaser or successor to the information may continue to use the information only if it has undertaken to use and disclose the information for the purposes for which it was originally collected and the information relates solely to the operation of the target business or relates to the objects of the business transaction. If the transaction is not completed or does not close, the recipient must destroy the personal information. Under the BC Act, there is also a requirement that where a transaction proceeds, an organization may disclose information without consent provided that any employees, customers, directors, officers and shareholders whose personal information is disclosed are notified that the transaction has taken place and that their personal information has been disclosed to the recipient.

Analysis and recommendations:

In order to anticipate the sale of franchise system and valuable customer lists in PIPEDA jurisdictions, the franchisor should ensure that it has obtained informed consents from all individuals whose personal data is collected by a franchisor or a franchisee. As indicated above, the principle is one of simple contractual consideration: in exchange for the delivery of certain products or services, the consumer agrees to provide financial consideration and its personal information for a certain number of limited purposes. If the purposes enumerated fail to include the subsequent transfer of the information to the franchisor for marketing purposes, for sale or lease to a data broker, or for subsequent assignment to a potential purchaser of the franchisor's business assets, then these activities simply cannot be undertaken without obtaining such express consents. At a very minimum a franchisor's website privacy policy should include the statement that personal information collected from customers may be transferred to purchasers of the franchisor's business.

In British Columbia and Alberta, provided the notice requirements of the Acts are complied with and providing that the statute is complied with in all other respects, prior notice of the transfer will not be required.

4. Franchisor's and franchisee's privacy obligations to employees

Currently, PIPEDA only imposes privacy obligations on employers of federally regulated undertakings. Private employers in those provinces without their own privacy legislation are not technically required to provide to their employees the protections legislated under PIPEDA where employee information is collected for the purposes of administering the employee relationship and not for a commercial purpose.

The Quebec Act, the BC Act and the Alberta Act all apply to employee information of provincially regulated businesses. The BC and Alberta Acts provide for the collection, use and disclosure of employee information without the employee's consent but upon prior notice to the employee provided that such collection, use and disclosure are reasonable for the purposes of establishing, managing or terminating the employee relationship.

Recommendations:

Employees should maintain strict privacy standards with respect to all collected personal information, including both consumer and employee information whether or not they are operating in a PIPEDA province or a jurisdiction in which “substantially similar” legislation has been enacted. Consents are often easily obtained at the outset of the employment relationship in application forms, employment agreements and confidentiality agreements, and can include all anticipated reasonable uses of personal employee information, such as criminal checks, credit checks, reference verification, performance evaluation and outsourcing of payroll.

D. Conclusion

Privacy compliance need not impose a burdensome cost to franchisors and franchisees. The establishment of a sound privacy policy, the institution and enforcement of good practices and the appointment of a diligent privacy officer are the minimum requirements. If in addition to the above a proactive, well-educated and privacy-sensitive approach is taken by franchises which collect, use and disclose personal information, then business disruptions due to privacy related matters will rarely, if ever, arise.