CHAPTER ❖ 5

Privacy Laws In Canada: Their Implications for Franchising and Marketing

PAUL JONES

I. Introduction To Privacy Issues

Knowledge about customer preferences and habits is very valuable information. The dramatic rise of e-commerce and the Internet, and the increased use of computers have transformed concepts of customer goodwill, and the ability of the retailer to collect, store and analyze information about customer preferences and habits.

Previously the customer goodwill attached to a brand was often intangible, something that could only be estimated based on sales. Now, depending somewhat on the product, brand managers can more easily develop methods to build customer databases and focus their efforts on improving the relationship with targeted customers. Customers are not as anonymous as they once were, and out of this has arisen the "new" science of customer relationship management.

While these possibilities have delighted marketing professionals, the same factors have contributed to heightened awareness and concerns amongst individuals worldwide regarding the information collected about them and its use. The first law attempting to regulate the collection and use of personal information in computer files was adopted by the German state

of Hesse (the area around Frankfurt-am-Main) in 1970,[1] and the first national law was adopted by Sweden in 1973.[2] This was followed by a law in France[3] and the development of the OECD Guidelines.[4]

In 1995 the European Union adopted what has come to be known as the E.U. Data Directive[5] to harmonize the national provisions within the European Union in order to facilitate transborder data flows within the Union. To ensure that the E.U. Data Directive would be effective, it provided that the transmission of personal information outside of the E.U. was only possible to countries where the law afforded similar protection to personal information. Procedures were also set out in the E.U. Data Directive for approving countries that had adequate data protection laws or for approving transfers on a case-by-case basis where data protection would be ensured by contract. As these provisions have significant implications for countries trading with the E.U., the adoption of the E.U. Data Directive has accelerated the adoption of privacy laws around the world, including in Canada.

As of January 1, 2004 the federal privacy legislation came into effect for transactions entirely within a province, and many Canadian retailers have had to adjust their sales methods.[6] In addition, privacy laws came into effect in British Columbia and Alberta on the same date. Québec has had a privacy law in effect since 1994.

Although the common law in the United States long ago developed the tort of invasion of privacy, the federal government in the United States has not yet moved to codify general principles for the protection of personal information. The United States is the centre of the global Internet industry, and many Internet companies are concerned about the effect that such laws

---

[1] Now part of Hessisches *Datenschutzgesetz* (HDSG) in der Fassung vom 7 Januar 1999.
[2] *Datalagen*, SFS 1973:289.
[3] *Loi No.-78-17 du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés.*
[4] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" as adopted by the Council of the Organization of Economic Co-operation and Development in September 23, 1980. Available on-line at <www.oecd.org/dsti/sti/it/seur/prod/PRIV-EN.HIM>.
[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October, 1995, available on-line at <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_595L0046.html>.
[6] It should be noted that PIPEDA came into effect for the interprovincial and international collection, use or disclosure of personal information on January 1, 2001. The reasons for the staggered implementation will be discussed later in this Chapter. Since January 1, 2004 there has been a much greater awareness of privacy issues among both businesses and consumers.

might have on their ability to develop e-commerce and Internet marketing. The U.S. Federal Trade Commission ("FTC") reversed itself in May of 2000[7] and recommended that Congress enact legislation to ensure the adequate protection of consumer privacy on-line, because voluntary codes were not seen to be working. Since then a deadlock has developed in Congress over the type of consent that should be required for the use of personal information for marketing purposes, and the degree of access to be afforded to consumers.

There have been laws passed in the United States to protect personal information in areas where it appears to be particularly sensitive, such as video rentals,[8] children,[9] financial information,[10] and health care information,[11] and the FTC has developed a voluntary standard for privacy policies described as "Notice, Choice, Access and Security".[12] The FTC has also prosecuted several Internet companies under section 5 of the *Federal Trade Commission Act*[13] for failing to comply with their own written privacy policies as posted on their website. More recently the FTC's Director of Consumer Protection has verbally warned that the FTC plans to make consumer privacy rights a higher priority.[14]

However in the United States the consent of the individual customer to the collection, use and disclosure of the customer's personal information for use in customer relationship management programs is still not required in most instances. The opposite is now true in Canada, Europe, Australia and many other countries.

---

[7] See Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress (Washington, DC, Federal Trade Commission, May 22, 2000).

[8] *Video Privacy Protection Act of 1988,* (the "Bork Bill"), 18 U.S.C. §2710.

[9] *Children's Online Privacy Protection Act*, ("COPPA"), 15 U.S.C. §§6501-6506, 6502(c), and 6505(d), and the *Children's Online Privacy Protection Rule,* 16 C.F.R. Part 312, in effect April, 2000.

[10] *Gramm-Leach-Bliley Act*, also known as the *Financial Services Modernization Act of 1999*, Pub. L. No. 106-102, 113 Stat. 1338 (1999), which became effective July 1, 2001.

[11] *Health Insurance Portability and Accountability Act of 1996* and the *Standards for Privacy of Individually Identifiable Health Information,* (the "Privacy Rule") promulgated by the U.S. Department of Health and Human Services as 45 CFR, Parts 1601 and 164, for compliance by April 14, 2003.

[12] First described in the FTC's report *Privacy Online: A Report to Congress*, in 1998.

[13] Title 15 U.S.C.

[14] Stefanie Olsen, "FTC: All eyes on consumer privacy", *CNET News.com*, June 10, 2004.

After a general discussion of the way in which privacy issues affect franchisors in particular, this Chapter will then discuss Canada's privacy laws, and the remedies available for breach of privacy. It will then return to the discussion of issues specific to franchising, including obtaining the appropriate form of consent, before finishing with a discussion of how to comply with Canada's privacy laws.

II. Franchising Issues

A franchise system is not a single entity in the eyes of the law. Rather it consists of a number of legal entities, bound together by contracts that require that all of these individual entities act in a somewhat coordinated way when selling a product or service, under a single trade-mark or brand owned by the franchisor. In other areas the franchisees retain varying degrees of autonomy. The application of privacy laws to the franchise structure results in two significant problems that do not arise for other retailers.

It is the franchisees in a system that have the day-to-day customer contact and thus accumulate knowledge about customer preferences and habits. Franchisors have traditionally dealt with this problem by, among other things, putting provisions in the franchise agreements that the franchisor owns the customer list, or at least requiring transfer of the list or other customer information to the franchisor. Now in Canada and Europe, notwithstanding such provisions, such information cannot be transferred without customer consent. Franchisees and dealers have used privacy laws to resist demands for such transfers.[15]

The second significant problem for franchisors first considering the effect of privacy laws on their systems will be whether privacy compliance standards will be set system wide and perhaps vigorously enforced by the franchisor, or whether franchisees will simply be required to comply with all relevant laws, and otherwise left to their own devices.

There are a variety of factors that will need to be taken into account in making this decision, including:

1. The nature of the product and/or services;

---

[15] Connie Gugliemo, "Ransom: Customer Data" *ZDNet.com*, October 8, 2000. When Motorola required its independent dealers in the U.S. to enter into a new form of agreement requiring them to collect and transfer to Motorola "valid end-user customer information" the dealers resisted citing privacy concerns.

2. The way marketing is currently being carried out;
3. The way marketing will need to be carried out in the future if use of the Internet continues to grow;
4. Who owns the customer lists; and
5. The risks of non-compliance.

There may also be employment issues and issues regarding the cross-border application of privacy laws.

A fundamental problem for franchise systems is that such systems are designed to present a common identification to the public and their customers, and yet retain the advantages of individual entrepreneurship and effort by being made up of separate legal entities. The common identity is maintained by use by the franchisees of only the trade-marks specified by the franchisors. Each franchise agreement is thus also a trade-mark license agreement.

Trade-marks are considered to indicate the source of the goods or services, and to assist the public and customers by reducing search costs when they are seeking goods or services of a particular type or quality. Accordingly, the Canadian *Trade-marks Act*[16] requires that such trade-mark licenses contain certain provisions to ensure that benefits to the public are not lost. Specifically, the owner of the trade-mark, or franchisor, must maintain "....direct or indirect control of the character or quality of the wares or services...."[17] failing which the trade-mark will be held to be non-distinctive. Courts have added the requirement that not only must the license agreement contain clauses allowing the owner to exercise such control, but the owner must in fact exercise the control, by, for example, conducting audits of the goods or services and the associated use of the mark.[18]

For a franchisor considering how to comply with privacy laws, one of the first steps will be to consider to what extent customers and/or the public see privacy compliance as part of the franchisor's goods and/or services, and therefore to consider the extent to which a common privacy compliance standard is expected for goods and services bearing the franchisor's trade-mark. The franchisor can then go on to consider other issues, such as the

---

[16] R.S.C. 1985, c.T-13.
[17] *Ibid.* at s. 50(1).
[18] See for example *Unitel Communications Inc. v. Bell Canada* (1995), 61 C.P.R. (3d) 12 (F.C.T.D.).

best way to market the goods and/or services through the system, and how that is affected by privacy compliance.

Franchisors will have to examine their compliance options in light of the balance struck between the benefits achieved through uniform marketing on the one hand, and both the costs of system wide implementation and maintenance, and the risk to the franchisor of liability for franchisee conduct on the other. To continue with this analysis the next step is to look at the structure of the privacy laws.

III. Privacy Laws

A. BASIC PRIVACY PRINCIPLES

Around the world different jurisdictions have developed different ways of describing or expressing the basic principles of their privacy legislation, but they all have similar elements. These elements may be described as follows:

1. Individuals must be given notice of the proposed collection, including use and disclosure, and the specific purposes.
2. In order for the data to be collected, used or disclosed, appropriate consent must be obtained with respect to the specified purposes.
3. The data collected must be protected by appropriate security.
4. The individual must have access to the data collected, and to details of its use and disclosure.[19]

Variations exist in the method of ensuring compliance. In the European Union, registration is required in order to maintain databases of personal information and the registrar may take an activist role in ensuring compliance with the privacy principles. In other jurisdictions the primary responsibility for ensuring compliance rests with individuals through use of the courts or an administrative tribunal.

Privacy legislation is based on what might be called a "contract" model. As with contracts, problems have developed with the nature of the consumer's understanding of the contract that is being proposed, the meaning of some of the terms, and the balancing of interests or fairness of the contract or consent. In traditional contract law these are often referred to

---

[19] For an alternative discussion of the basics of fair information practices see Anne Cavoukian and Tyler J. Hamilton, *The Privacy Payoff: How Successfully Businesses Build Customer Trust* (Toronto: McGraw-Hill Ryerson, 2002) at pp. 44-45.

as problems of "unconscionability" or "good faith". Thus significant variations are developing between jurisdictions with respect to the limitations or restrictions that they impose on privacy contracts. For example, as will be discussed later in this Chapter, a number of European jurisdictions prescribe various types of personal information that must be considered sensitive, and either require more explicit consent, or prohibit collection of such personal information altogether.

The United States FTC, as noted above, has set out its privacy principles most succinctly as "Notice, Choice, Access and Security". In the United Kingdom, the provisions of the E.U. Data Directive were summarized in eight data protection principles.[20] Canada has chosen to use ten privacy principles, adopted from the Canadian Standards Association ("CSA") Model Code,[21] a voluntary code that had been developed by the private sector. A description of the ten principles is provided in the next section.

B. CANADA'S PRIVACY LAWS

The nine Canadian provinces with common law based legal systems do not have a tradition of protecting privacy. In contrast to the protections developed in civil law countries such as France, in the United Kingdom the basic common-law principle was that there is no right to privacy nor any action for invasion of privacy per se. In Canada, while the courts have never specifically stated the English position, they have been reluctant to find liability on a privacy right alone. Often, the issue has been avoided by the use of more established categories of torts.

---

[20] See Schedule 1 of the *Data Protection Act 1998* (Chapter 29, London: The Stationery Office Ltd.) The eight principles are: 1) personal data shall be processed fairly and lawfully; 2) personal data shall be obtained for lawful and specified purposes; 3) personal data shall be adequate, relevant and not excessive to the purposes; 4) personal data shall be relevant and kept up to date; 5) personal data shall not be retained for longer than is necessary; 6) personal data is to be processed in accordance with the rights in the legislation; 7) security measures shall be implemented; and 8) personal data shall not be transferred outside the E.U. unless adequate protection is afforded.

[21] The Code is now Schedule 1 of PIPEDA – "Principles Set Out in the National Standard of Canada Entitled Mode Code for the Protection of Personal Information, CAN/CSA-Q-830-96".

1. Federal – PIPEDA

Unlike the U.S., but like most of the other developed countries in the world, Canada has chosen to implement a general private sector personal information protection law, the federal *Personal Information Protection and Electronic Documents Act*[22] (also known as "PIPEDA"). The objectives of the federal government were to strengthen e-commerce in Canada and to provide a legal framework that would comply with the E.U. Data Directive. Canadian companies did not appear to have the same concerns as their American counterparts regarding restrictions on use of consumer information, possibly because many already adhered to a voluntary code developed by the direct marketing industry and others in conjunction with the Canadian Standards Association, and because Québec has had privacy protection since 1994.

The basic principles of PIPEDA are the same as most privacy laws, and these are described and commented upon in the first section below. Other issues, such as the constitutionality of PIPEDA, and its provisions for enforcement, often have a significant effect on the application of PIPEDA to a particular matter, and will be discussed in this section. These issues present problems in the interpretation of PIPEDA that may well lead to foreign counsel receiving conflicting advice from Canadian counsel. These latter sections are intended to assist foreign counsel in understanding the source of the difficulties in interpretation.

(a) Canada's Ten Privacy Principles

The ten privacy principles set out in Schedule 1 to PIPEDA, the CSA Model Code, are the substantive provisions of PIPEDA, notwithstanding the fact that they are drafted in a form more suited to a voluntary code. The statute itself has the exceptions to the substantive requirements, and must be referred to when reading the provisions of the Schedule.

Practice Note

Because of PIPEDA's unusual structure, the easiest way to read it is to read Schedule 1 first, and then to read the actual statute that contains the exceptions and qualifications.

---

[22] S.C. 2000, c. 5, as amended by S.C. 2000, c.17, s. 97.

The result has been that PIPEDA is unusually difficult to interpret. The language of the CSA Model Code, as a voluntary industry standard, is inherently vague. While some provisions, most notably the exceptions for obtaining consent, have been clarified, other important concepts, such as what is "sensitive" information, are left to the courts to determine. Even the process for seeking remedies is not clear, making it difficult to assess the risks of non-compliance. To add to the confusion, different lawyers often give differing opinions when interpreting PIPEDA. Ultimately clients will have to determine their own comfort level in difficult areas.

One of the more interesting provisions of PIPEDA is a limitation on the purposes for which an organization may collect, use or discloses personal information.[23] Such purposes must be ones that "... a reasonable person would consider appropriate in the circumstances." This restriction has been frequently cited by the federal Privacy Commissioners in their findings.

Principle 1 – Accountability

This Principle generally requires the designation of an individual or individuals who are accountable for the organization's compliance with PIPEDA. The organization is specifically held responsible for information that has been transferred to a third party for processing, which must be protected by contractual means. Organizations are required to implement policies and practices to give effect to the principles, including training staff. This Principle remains as set out in the CSA Model Code, and has not been modified by PIPEDA.

Principle 2 - Identifying Purposes

The purposes for which personal information is collected must be identified to the individual at or before the time that it is collected. Once this has been done, the personal information cannot be used for a new or further purpose without the further consent of the individual.

Section 5(3) of PIPEDA provides that "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances". The Privacy Commissioner sees this section as providing an outer limit on the purposes that may be used by an organization to justify data collection, use or

---

[23] *Supra* note 22 at s. 5(3).

disclosure. Obtaining the consent of the individual for the collection of personal information outside of these limits may be insufficient for compliance.

This Principle is also modified by Principles 4 and 5 regarding limiting collection, use, disclosure and retention.

Principle 3 – Consent

This Principle is generally regarded as the key to the protections in PIPEDA, and will be further discussed later in this Chapter.

Generally speaking, personal information cannot be collected, used or disclosed without the knowledge or consent of the individual, unless there is a specific exemption provided for in section 7 of PIPEDA. An organization may not, as a condition of the supply of a product or service, require such consent beyond what is required for a legitimate fulfilment of the transaction. The form of consent may be explicit or implicit, or "opt-in" or "opt-out", depending upon the sensitivity of the information. The concept of "sensitivity" is somewhat problematical and it is discussed further in the next section. Because of this, it is always more prudent to try to obtain written consent. Finally, consent can be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice.

The former federal Privacy Commissioner made his antipathy to opt-out consent abundantly clear in his findings regarding Air Canada's Aeroplan Frequent Flyer Program, released March 20, 2002.

> "I should begin by making it clear that, like most other privacy advocates, I have a very low opinion of opt-out consent, which I consider to be a weak form of consent reflecting at best a mere token observance of what is perhaps the most fundamental principle of privacy protection. Opt-out consent is in effect the presumption of consent – the individual is presumed to give consent unless he or she takes action to negate it. I share the view that such presumption tends to put the responsibility on the wrong party. I am also of the view that inviting people to opt-in to a thing, as opposed to putting them into the position of having to opt-out of it or suffer the consequences, is simply a matter of basic human decency.
>
> Accordingly, while acknowledging that the *Act* does provide for the use of opt-out consent in some circumstances, I intend, in this and all future deliberations on matters of consent, to ensure that such circumstances remain limited, with due regard both to the sensitivity of the information at issue and to the reasonable expectations of the individual. In other

words, in interpreting Principle 4.3.7, I intend always to give full force to other relevant provisions of the *Act*, notably 4.3.4, 4.3.5 and 4.3.6 and section 5(3)."[24]

Since the Air Canada finding there has been the appointment of a new Privacy Commissioner, and a more recent finding (#207)[25] has specified a number of conditions to be met for an organization to justify reliance upon the opt-out form of consent. They are:

1. The personal information must be clearly non-sensitive in nature and context.
2. The information-sharing situation must be limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.
3. The organization's purposes must be limited and well-defined, stated in a reasonably clear and understandable manner, and brought to the individual's attention at the time the personal information is collected.
4. The organization must establish a convenient procedure for easily, inexpensively, and immediately opting out of, or withdrawing consent to, secondary purposes and must notify the individual of this procedure at the time the personal information is collected.

Practice Note

As suggested by the Privacy Commissioner, one of the keys to limiting complaints is to have convenient, easy-to-use, inexpensive methods available to individuals to allow them to opt-out or otherwise withdraw their consent.

Care must be taken in reading the specific sections of this Principle in the Schedule because it is extensively revised by section 7 of PIPEDA, which provides the specific and only exceptions from obtaining consent for the collection, use, and disclosure of personal information.

---

[24] Office of the Privacy Commissioner of Canada, "News Release: Ottawa, March 20, 2002," online: Aeroplan Frequent Flyer Program<http://www/privcom.gc.ca/media/nr-c/02_05_b_020320_e.asp>.

[25] Commissioner's Finding 207 – Aug. 6, 2003 – Privacy Commissioner (PIPEDA Act Case Summary #207)

Principle 4 - Limiting Collection

This Principle provides that the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Purposes need to be reasonably specific. Information must be collected by fair and lawful means.

This principle is not modified by PIPEDA.

Principle 5 - Limiting Use, Disclosure and Retention

This Principle provides that 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 it is necessary for the fulfilment of those purposes. Organizations must develop guidelines with maximum and minimum retention periods.

This Principle is also modified by section 7 of PIPEDA.

Principle 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.

However, the extent to which this must be implemented depends upon the use of the information, taking account of the interests of the individual. While this Principle is vaguely worded, it is relevant mainly to organizations that collect information to make decisions that may affect the subject individual adversely.

This Principle is not modified by PIPEDA.

Principle 7 – Safeguards

Personal information is to be protected by security safeguards appropriate to the sensitivity of the information. As with Principle 3 - Consent, "sensitivity" is a key concept. The purpose of the safeguards is not just to protect against theft, but also to protect against unauthorized access, disclosure, copying or use. The methods of protection should include physical measures, such as locked filing cabinets and restricted access; organizational measures, such as security clearances and access on a "need-to-know" basis; and technological measures such as passwords and encryptions. How many organizations currently maintain such safeguards? How many think they should? What would be the cost of implementation?

Practice Note

Identity theft is seen as having significant potential privacy liability for organizations. Also the promises made in privacy policies and on web sites regarding security have been found not to match actual practice. Franchisors should pay particular attention to the security that they provide to personal information of customers. The loss of a laptop with customer payment details on it would be a significant event.

Principle 8 – Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. This Principle effectively requires the use of privacy statements by organizations operating in Canada, on websites, or on other material, including printed material, through which they collect personal information. It also requires that the privacy policy developed pursuant to Principle 1 be made available to individuals. Specifically the information to be made available shall include:

1. The name or title and the address of the person who is accountable pursuant to Principle 1;
2. The means of gaining access to personal information held by the organization;
3. a description of the type of personal information held by the organization, including a general account of its use;
4. a copy of any brochures or other information that explain the organization's policies, standards or codes; and
5. what personal information is made available to related organizations such as subsidiaries.

Practice Note

While many franchisors already have consent wording on their franchisee application forms, the wording probably does not comply with all the requirements of Principle 8.

Principle 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.

This right of access is limited by the provisions of sections 8 and 9 of PIPEDA, which set the terms for requesting access, and prescribe when access is prohibited,[26] or may be refused by the organization holding the information.[27]

In the United States, the principle of access is one of the major concerns of those opposed to privacy legislation, because of the anticipated cost of complying with requests. Experience with privacy legislation in the United Kingdom tends to suggest that estimates of a deluge of requests, many of which are frivolous, are quite unfounded. But based on the experience in Québec, requests to see personal information are now an expected part of a dispute with an employee or other individual.

In PIPEDA, such disclosure includes an account of the use that has been made of the information, and an account of the third parties to which the information has been disclosed. Such disclosure can be expensive to make if the files containing such information have not been properly structured in advance to record and summarize such information as use occurs.

The full cost of making such disclosure cannot be recovered from the person making the request. Paragraph 4.9.4 of this Principle provides that responses are to be at minimal or no cost to the individual.[28] Section 8(6) further specifies that the individual may be required to pay only if the individual is notified in advance of the approximate cost and agrees to pay.

Principle 10 - Challenging Compliance

An individual shall be able to address a challenge concerning compliance to the individual accountable for the organization's personal information.

---

[26] *Supra* note 22 at s. 9(1).
[27] *Supra* note 22 at s. 9(3).
[28] For a discussion of the interpretation of the provisions regarding costs see Paul Jones, "Privacy Law: A New Era", (paper presented to the 12th Annual Meeting of the Canadian Corporate Counsel Association in Halifax, August 2000), [unpublished] at pages 16 and 17.

(b) Constitutionality and Jurisdiction:

Unfortunately, privacy and personal information are not mentioned in the *Constitution Act, 1867*.[29] While this would suggest that it is residually a provincial matter, with today's technology, much information is transferred electronically across provincial or national boundaries, which provides a basis for federal jurisdiction. Personal information and privacy are thus areas where there is often clearly overlapping federal and provincial jurisdiction, or concurrency.

Unlike the U.S. Constitution, which allows such concurrent jurisdictions to exist, Canada's constitutional structure is based on a notion of exclusive areas of jurisdiction. If the Canadian federal government passes a law in a subject matter that is in the provincial jurisdiction, the law can be challenged as being *ultra vires* the federal government, and therefore invalid.

Accordingly because of Canada's constitutional division of powers the federal government was limited in the scope of the privacy law that it could enact. The provinces have exclusive jurisdiction over matters of private property and civil rights, while the federal government has a general power to regulate trade and commerce.

More importantly, the provinces, pursuant to section 92(7)[30] of Canada's *Constitution Act, 1867*,[31] have exclusive jurisdiction over charitable and health related organizations. Accordingly, the application of PIPEDA is limited to organizations and transactions within the ambit of the federal constitutional powers.[32] The federal government relied primarily on the trade

---

[29] (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II. No. 5.

[30] *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c.3, s.92(7); reprinted in R.S.C. 1985, App. II, No.5. The provision reads as follows:
" The Establishment, Maintenance, and Management of Hospitals, Asylums, Charities, and Eleemosynary Institutions in and for the province, other than Marine Hospitals."

[31] (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II. No. 5.

[32] Section 4(1) of PIPEDA provides that PIPEDA applies to personal information that: the organization collects, uses or discloses in the course of commercial activities; or is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.
The definition of the second group of organizations to which PIPEDA applies, the federal works or undertakings, is borrowed from the Canada Labour Code, and there is a significant body of case law determining whether federal or provincial labour laws apply to a particular group of employees. A quick test as to whether an organization falls into this group is to ask whether its employees are governed by federal or provincial labour law.

and commerce power in enacting PIPEDA, and this has focused the application of PIPEDA on commercial activities.

There is no policy basis in privacy law for limiting the application of such laws to commercial activities and excluding hospitals and charities. Neither the E.U. Data Directive nor Québec's privacy legislation distinguish between commercial and non-commercial uses of information. It is anticipated that this constitutional division of powers will make the interpretation of PIPEDA particularly problematic for marketing initiatives in the health and non-profit sectors.

Constitutional issues also led to another anomaly in the drafting of PIPEDA, namely the delay in its application to matters within a province until January 1, 2004.[33]

The federal trade and commerce power has an inherent conflict with the provincial jurisdiction over property and civil rights within a province. Initially, the courts narrowed the federal trade and commerce power[34] but more recently *General Motors v. City National Leasing*[35] established a new test for determining the appropriate exercise of the trade and commerce power by the federal government. The elements of the test were:

1. the presence of a general regulatory scheme;
2. the oversight of a regulatory agency;
3. a concern with trade as a whole, rather than with a particular industry;
4. the legislation should be of a nature that the provinces jointly or severally would be constitutionally incapable of enacting; and

---

Determining the boundaries of the first group, organizations that undertake "commercial activities" is more difficult. PIPEDA defines this term as follows:
"commercial activity" means 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".
The definition appears to have been broadly drafted to specifically catch non-profit and charitable organizations trading in membership or fundraising lists.

[33] PIPEDA was passed by Parliament on April 13, 2000. It initially came in to effect for organizations clearly within the federal jurisdiction on January 1, 2001. Thus most of its cases to date arose out of banks, interprovincial transportation companies, such as airlines and railroads, and telecommunications companies.

[34] *Citizens' Insurance Co. v. Parsons* (1881), 7 App. Cas. 96. See Peter W. Hogg, *Constitutional Law of Canada – Looseleaf Edition* (Toronto: Carswell, 1997) at page 20-2 for a discussion of this case.

[35] [1989] 1 S.C.R. 641.

5. the failure to include one or more provinces or localities in a legislative scheme would jeopardize the successful operation of the scheme in other parts of the country.

As was illustrated by the concerns of the European Union with the possible avoidance of the personal information protection provided by E.U. Data Directive by the transfer of personal information outside the E.U., privacy protection in the age of computers and the Internet requires legislation that deals with interprovincial and international transfers, which are the exclusive jurisdiction of the federal government. Thus condition four is satisfied, and possibly condition five of the test noted above. To ensure compliance with the fifth condition, the provinces were given three years to pass their own privacy legislation.

The constitutional status of PIPEDA is still an open question. While a decision of the Québec Superior Court has held that the Commission d'accès à l'information du Québec does not have jurisdiction over a federal undertaking such as Air Canada,[36] in December of 2003 the government of Québec asked the Québec Court of Appeal to consider the question of whether PIPEDA is within the federal jurisdiction.[37]

(c) Remedies:

The remedies provisions of PIPEDA deserve careful consideration. The role of the Privacy Commissioner of Canada has been circumscribed in that the "findings" (to use the term adopted by the Commissioner) are not binding on the parties, and consequently there is no right of appeal from the findings of the Commissioner in a particular matter. The organization against whom the complaint is made has the option of simply ignoring the Commissioner's report.

Further, in section 24 of PIPEDA the Commissioner has been given a mandate "... to foster public understanding, and recognition of the purposes,..." of PIPEDA. Thus the Commissioner's role is somewhere between that of an ombudsperson, a finder of fact, and an advocate for privacy. That this role does not include making binding decisions should be

---

[36] *Air Canada c. Constant et l'CAI*, JG1793, No. 500-05-074681-022, 3 septembre, 2003.
[37] The specific question is " Does Part 1 of the *Personal Information Protection and Electronic Documents Act* (S.C. 2000, ch. 5) exceed the legislative competence that the *Constitution Act of 1867* confers on the Parliament of Canada?"

taken into account when considering the importance to be attached to the actions of the Commissioner.

Section 11(1) of PIPEDA provides that an individual may file with the Commissioner a written complaint against an organization for contravening the privacy portions of PIPEDA. The "Commissioner" is the Privacy Commissioner appointed under section 53 of *Privacy Act*, the law regulating the information held by the Federal Government.

The Commissioner may then investigate complaints in an attempt to resolve them by mediation and conciliation. The Commissioner is required to produce a report within one year of the filing of the complaint that contains the Commissioner's findings and recommendations among other things. However the Commissioner is not required to prepare a report if the Commissioner is satisfied that:

> (a) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available; [or]
>
> (b) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province.[38]

Based on the use of the word "may" in section 11(1), and the above-noted conditions for not issuing a report in section 13(2) as cited above, some lawyers are of the opinion that the remedies prescribed in PIPEDA are not the only remedies available for a breach of the provisions of PIPEDA. For example, it may be possible to bypass the Privacy Commissioner and commence an action directly.

Finally, section 14(1) provides that a complainant may, after receiving the Commissioner's report, apply to a Federal Court Trial Division for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and is the subject of certain specific sections of Schedule 1 to PIPEDA, or PIPEDA itself. Pursuant to section 16, the Federal Court then may, in addition to other remedies it may give, provide the following remedies:

---

[38] See, for example, the contrasting decisions with regard to employment matters in *L'Ecuyer c. Aéroports de Montréal*, 2003 FCT 573 (released May 13, 2003); upheld on appeal 2004 CAF 237 (released June 17, 2004) and *Eastmond v. Canadian Pacific Railway and the Privacy Commissioner of Canada*, 2004 FC 852 (released June 11, 2004).

(a) order an organization to correct its practices in order to comply with PIPEDA;

(b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and

(c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

The Commissioner also has the power to audit personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening a provision of PIPEDA. The results of this audit may be included in its Annual Report.

Pursuant to section 20(2), the Commissioner may make public any information relating to the personal information management practices of an organization if the Commissioner considered that it is in the public interest to do so. The Commissioner may further authorize disclosure of information in the course of a hearing before the Federal Court. However, to date the Commissioner has only made available copies of anonymized summaries of the findings under PIPEDA, a practice that has led to some concern amongst privacy advocates.

Finally, pursuant to section 21(1) there are provisions protecting whistle blowers, that is people who have reasonable grounds to believe that an organization has contravened, or it intends to contravene, a provision of the PIPEDA and who notify the Commissioner.

(d) Summary

It is often difficult for lawyers to provide clients with precise advice on the requirements of PIPEDA, because of issues such as the nature of its drafting and the blurring effect of the unresolved constitutional questions. Further the Commissioner's "findings" must be used with caution. They are at best a guide as to how the Commissioner might react to a particular situation.

In these circumstances clients are often advised to take business considerations into account when making decisions on how to implement PIPEDA. As a result of the recent coming into force of privacy laws across Canada, consumers are more aware than ever that they have some form of privacy rights. Needless to say, they are blissfully unaware of the constitutional and other limitations on these rights. Accordingly, keeping a

customer satisfied with respect to privacy may sometimes require more than simply complying with PIPEDA.

2. Québec

In civil matters such as privacy, Québec follows the civil code model as found in France, and the *Code civil du Québec*,[39] (the "Civil Code") Article 35, provides as follows:

> Art. 35:
>
> Toute personne a droit au respect de sa réputation et de sa vie privée.
>
> Nulle atteinte ne peut être portée a la vie privée d'une personne sans que celle-ci ou ses heritiers y consentent ou sans que la loi l'autorise.
>
> 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.

Article 36 goes on to illustrate items that might be considered as invasion of the privacy of a person. They include entering or taking anything in a person's dwelling; intentionally intercepting or using the person's private communication; appropriating or using the person's image or voice while the person is in private premises; keeping the person's private life under observation by any means; using the person's name, image, likeness, or voice for a purpose other than providing legitimate information to the public; or using the person's correspondence, manuscripts or other personal documents.

To expand upon the provisions of the Civil Code, in 1993 Québec also passed the *Loi sur la protection des renseignements personnels dans le secteur privée.*[40] ("Québec's Private Sector Law") Under this law, which came into effect January 1, 1994, there is no general obligation for registration, however, pursuant to section 70 of the Québec's Private Sector Law, every personal information agent, being the person who, on a commercial basis, personally or through a representative, establishes files on

---

[39] L.Q. 1991, c. 64.
[40] L.R.Q., c. P-39.1.

other persons, must register with the Commission d'accès à l'information du Québec. Generally this section affects credit agencies.

The Québec's Private Sector Law sets the standards with respect to the collection and use of personal information, including having a defined purpose or object; collecting only the necessary information; informing the person from whom the file is established; and obtaining consent for transferring such file to a third party.

On November 19, 2003[41] the federal Government of Canada declared that the Québec's Private Sector Law is substantially similar to PIPEDA in terms of the extent to which it protects personal information. However, there are some important differences for franchisors.

The Québec's Private Sector Law has notice requirements in article 8 that are broader than those under PIPEDA's Principle 8. Individuals must be advised of the categories of persons within the organization who will have access to the information, and the place where the file will be kept. Article 20 explicitly limits the access of employees and agents of a corporation to that which is needed in the performance of their duties.

Franchisors considered to be carrying on business in Québec and wishing to transfer information relating to Québec out of the province will have obligations under article 17 to take all reasonable steps to ensure that either the information will not be used for purposes not relevant to the object of the file, or disclosed to third persons without consent, or in the case of nominative lists, that the individuals have a valid opportunity to have their name deleted from the list.

Article 22 of the Québec's Private Sector Law provides for the transfer to a third party, without the consent of the individuals concerned, of a "liste nominative" if by contract the third party is prohibited from using or disclosing the list for purposes other than commercial or philanthropic prospection; if the individuals have had a valid opportunity to opt-out of such transfer, and if the communication does not infringe on the privacy of the persons concerned. Nominative lists are lists of names, addresses or telephone numbers of individuals.

Care must be taken in relying upon the exemption if the source of the list would reveal significant or sensitive personal information about the individuals on the list. If the list was of persons who had visited a web site for AIDS sufferers, presumably the transfer of such list would not comply

---

[41] S.O.R./2003-374.

with the third condition, that the privacy of the individuals on the list not be infringed.

In such circumstances, consent to the communication or use of the personal information must be obtained pursuant to article 14 of the Québec's Private Sector Law. Article 14 provides that such consent must be "...manifeste, libre, éclairé et donné à des fins spécifiques."[42] The federal Privacy Commissioner found that such requirement is at least as strong as the requirement in PIPEDA, and in practice it appears that the term "manifeste" is more likely to require explicit consent than implied consent. In other words, it appears that reliance on implied consent, and thus the use of "opt-out" provisions, is more restricted in Québec.

Practice Note

When doing business in Québec it is more likely that explicit or written consent will be required.

Individuals or groups through a representative, or any interested person, may submit disputes to the Commission, who as prescribed by Article 55 may make orders to protect the rights of the parties and rule on any issue of fact or law. The Commission, however, is not considered to have the power to award damages. A decision by the Commission becomes the equivalent of a decision of the Superior Court when filed with the court. Decisions on matters of fact are final, but an appeal may be had, with leave, on matters of law and jurisdiction. The decisions of the Commission are available, in the language in which they were rendered (which is primarily French), on line at http://www.cai.gouv.qc.ca.

The Québec's Private Sector Law has been in force since January 1, 1994 and it is generally considered to be working well. On December 6, 2002 the Commission d'accès à l'information du Québec presented its 5 year report to the Québec Government.[43] Almost the entire report dealt with

---

[42] This is translated by the Québec government as " ...manifest, free, and enlightened, and must be given for specific purposes" in the English version of the law.

[43] Commission d'accès à l'information du Québec, Une Réforme de l'Access à l'Information – Le Choix de la Transparence: Rapport sur la mise en oeuvre de Loi du secteur privée sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de Loi du secteur privée sur la protection des renseignements personnels dans le secteur privé (Québec: Commission d'accès à l'information du Québec, 2002). Available online at www.cai.gouv.qc.ca.

problems with the public sector legislation, rather than the Québec's Private Sector Law.

3. British Columbia and Alberta

Ontario was the first province to commence a consultation process for its own privacy law after the coming into force of PIPEDA, but the law was never introduced in the Legislature. Only British Columbia and Alberta have passed laws to specifically take advantage of the provincial exemption provisions of PIPEDA. The two provinces collaborated closely on the drafting of their laws, with the intent of establishing a model law that other provinces could use. In both provinces the law is called the *Personal Information Protection Act*,[44] and both laws came into effect on January 1, 2004. However, as of the date of writing, the Federal Government had not yet issued the necessary Order-in-council (decision) exempting transactions within these provinces from the application of PIPEDA. Notice of intent to do so has been advertised by the federal government in its official publication, the Canada Gazette.[45]

The principles embodied in the design of these laws is the same as PIPEDA, however unlike PIPEDA, the laws do not use the CSA Model Code as a schedule. Rather, the principles in the CSA Model Code have been integrated directly into one overall law. In this regard, these laws are easier to read than PIPEDA. The laws also differ from PIPEDA in a number of other ways, motivated primarily by an effort to avoid errors in PIPEDA or areas where PIPEDA is not regarded as particularly workable. The main differences (apart from the provisions for remedies) may be summarized as follows:

1. Implicit Consent – the concept is defined in section 8 in both laws. PIPEDA does not explicitly set standards with respect to consent.
2. Existing Databases – both laws provide that information collected before the laws came into force may continue to be used for the purposes for which it was originally collected.[46] PIPEDA makes no

---

[44] British Columbia: *Personal Information Protection Act*, S.B.C. 2003, c. 63 ("B.C. Act"); Alberta: *Personal Information Protection Act*, S.A., Ch. P-6.5 ("Alberta Act").
[45] Canada Gazette, Part I, Saturday, April 10, 2004; Vol. 138, No. 15.
[46] B.C. Act, *supra* note 44 at ss. 3(2)(i), 14(b) and 17(b); Alberta Act, *supra* note 44 at s. 4(4).

special provisions for existing databases, which has led to some significant compliance concerns.[47]

3. Employees – both laws define "employee personal information", and provide that consent is not required for the collection, use or disclosure of such information provided that it is " ...reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual", and the employee is notified of the practice in advance. PIPEDA requires the consent of the employee.
4. Unincorporated Associations – both laws provide that unincorporated associations may be considered an "organization" for the purpose of the law. PIPEDA simply states that an "organization" includes an association, a partnership, a person and trade union. In practice the Privacy Commissioner of Canada has regarded separate legal entities as separate organizations. A franchise system is an unincorporated organization.
5. Exceptions with Respect to Investigations – Both laws provide for the collection, use and disclosure of personal information without consent for a broader range of investigatory purposes than is allowed under PIPEDA.
6. Sale of Business Assets – Both laws allow for the disclosure without consent of the personal information of customers, employees, offices, directors and shareholders as part of the transfer of the assets of the business, under certain conditions. It is considered that these provisions were omitted from PIPEDA in error.

Something that is not clarified in these laws is the standard for determining when a provincial law applies and when PIPEDA applies. The British Columbia law simply states that they do not apply if PIPEDA applies.[48]

---

[47] The Office of the Privacy Commissioner of Canada has responded to these concerns by issuing a Fact Sheet on July 27, 2004 entitled "Best Practices for dealing with pre-PIPEDA personal information (grandfathering)". It is available from the Privacy Commissioners web site at <http://www.privcom.gc.ca/fs-fi/02_05_d_22_e.asp.>

[48] B.C. Act, *supra* note 44 at s. 3(2)(c). On July 27, 2004 the Information and Privacy Commissioner for Alberta posted a document entitled *Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Acts(PIPAs)*, that had been prepared in consultation among the offices of the privacy

The differences between these laws and PIPEDA may be important for franchisors if franchisees are left to develop their own privacy policies. The initial collection and use of the individual customers' information will be subject only to the provincial laws, if, as is likely, such collection is carried out entirely within a province. However, any transfer of the information to the franchisor, even with the consent of the individual, would be governed by PIPEDA, assuming that the transfer would cross a provincial or national boundary.

It should also be noted that in British Columbia and Alberta the enforcement of the laws will be markedly different from the enforcement under PIPEDA. As noted earlier, the federal Privacy Commissioner has no power to issue a decision that binds the parties. Further, to date the Privacy Commissioner has generally released only anonymous summaries of his "findings". However, in British Columbia and Alberta the privacy commissioners have the power to issue binding orders.[49] Further, David Loukidelis, British Columbia's Information and Privacy Commissioner, has publicly stated that he will publish his decisions in full, and not anonymously.[50] But these provincial privacy commissioners do not have the power to award damages. Both laws provide that once a commissioner's order against an organization becomes final, the individual affected by the order has a cause of action against the organization for damages for actual harm that the individual has suffered.[51] Under PIPEDA, an individual seeking damages must initiate an action in Federal Court.

---

commissioners of Alberta, British Columbia and Canada. It takes the approach that were more than one law might apply, the substance of the transaction and the subject of the complaint would be considered. It is possible, if a complaint involves various breaches, that more than one privacy office would have jurisdiction.

[49] B.C. Act, *supra* note 44 at s. 52; Alberta Act, *supra* note 44 at s. 52.

[50] David Loukidelis, "Thoughts on Private Section Privacy Regulation", November 24, 2003. Available from the web site of the Office of the Information and Privacy Commissioner for British Columbia at <http://www.oipc.bc.ca/sector_private/pubs_speeches.htm>.

[51] B.C. Act, *supra* note 44 at s. 57(1); Alberta Act, *supra* note 44 at s. 60(i).

Practice Note

Enforcement is likely to be more formal in British Columbia and Alberta than in the other English-speaking provinces that are under PIPEDA (the federal law).

4. Other Provinces

In provinces other than Québec, British Columbia and Alberta, PIPEDA generally came into effect with respect to the collection, use of disclosure within those provinces on January 1, 2004. However for constitutional and drafting reasons, most commentators feel that PIPEDA does not apply to employment relations within a province (other than for federally regulated businesses), as well as to charities and some aspects of health care. Currently, no other provinces have announced plans to adopt a privacy law of general application so as to obtain exemption from the application or PIPEDA.

Ontario has adopted a specific privacy law for the health sector, and there are existing health specific laws in Alberta, Manitoba and in Saskatchewan. There are other private sector privacy laws that will be discussed in the next section on remedies and enforcement.

5. Remedies and Enforcement

In evaluating the costs of complying with a law, it is generally useful to examine the remedies available for breaches of the law, in order to better understand the risks associated with the various steps required for compliance. Certainly in previous Canadian efforts to provide some degree of privacy protection, the costs associated with enforcing privacy rights have proved to be a significant deterrent to the enforcement and development of the law.

Canadian courts have never specifically stated what has been said in England, that there is no common-law right of privacy, nor any action for invasion of privacy *per se*. However they have been reluctant to find liability on such right alone. Often the issue has been avoided by use of more established categories of torts. There is always the possibility that a court will sometimes stretch the scope of a particular tort or will interpret

legislation in such a way as to effectively find a remedy for an invasion of privacy.[52]

Now that PIPEDA or a substantially similar privacy law is in effect across Canada, it may be more likely that a court will decide that there is a private right of action for invasion of privacy, in addition to any statutory rights provided, as noted earlier, particularly with respect to PIPEDA. The importance of a private right of action lies in the use of the courts and their ability to award damages. As noted above, in Canada privacy commissioners can at the most make rectifying orders, but cannot award monetary compensation that might offset the costs of bringing the complaint. Damages can also have a greater effect on compliance.

As noted earlier, under PIPEDA the Federal Court can award damages, including damages for humiliation. This is a type of damage that generally depends on the facts of the particular case, and for which it is not generally appropriate to set a fixed rule as to the quantum. The humiliation factor is often mentioned in wrongful dismissal and in libel and slander cases, but it is not easy to distinguish the amounts awarded with respect to this factor from the overall award.

Based on the limited case law available, it appears that the damages for simple invasion of the privacy of one individual in plain contravention of the statute, with minimal humiliation, would be in the neighbourhood of C$500 to C$2,000.

(a) Concurrent Remedies in Statute and Common Law

An example of the concurrent use of statutory and private remedies can be found in Québec. As noted earlier, Québec has privacy protection both in Articles 35 to 41 of the Civil Code and its *Loi sur la protection des renseignements personnels dans le secteur privé*. The law is enforced by the Commission d'accès à l'information du Québec. Persons having a concern regarding access to or rectification of personal information, or the deletion of personal information, may make an application to the Commission for the examination of the disagreement. The Commission has the power necessary for the exercise of its jurisdiction and may make any order it considers appropriate to protect the rights of the parties and rule on any issue or fact or law. In particular, it may order an organization to communicate, rectify or

---

[52] Examples of such cases are *MacIssac v. Beretanos* (1971), 25 D.L.R. (3d) 610 at 614 (B.C. Prov. Ct.) and *Robbins v. C.B.C.* (1958), 12 D.L.R. (2d) 35 (Que. C.S.).

not disclose personal information. The decisions of the Commission may be appealed to the Québec Court of Appeal.

Separately the Commission may, on its own initiative, or following a complaint, make an inquiry into the practices of an organization with respect to personal information. After calling such an inquiry, it may recommend or order the application of such remedial measures as are appropriate to ensure the protection of personal information.

There is no explicit right to damages in the Québec's Private Sector Law, and the Commission is not in the habit of awarding damages. Accordingly those seeking financial compensation for a breach of their privacy rights in the province of Québec have proceeded by way of a tort claim in a civil action. This is similar to the principle in English tort law that breach of a duty provided by a statute, if it results in damage to an individual, is a tort for which an action for damages will lie if there is no remedy, or no adequate remedy, in the statute itself. No action will lie if on a true construction of the statute it is held that the intention of the legislature in creating a duty is that some remedy other than tort, civil or criminal, shall be the only one available. With respect to PIPEDA, this issue has not yet arisen.

A private action in tort, based on a statutory right, was the approach used in *Aubry c. Les Éditions Vice Versa Inc.*[53] This particular action arose prior to the coming into force of the present version of the Civil Code or the Québec's Private Sector Law. It therefore was decided on the cases developed under the *Code Civil du Bas Canada* and the provisions of the *Québec Charter of Human Rights and Freedoms.*

In *Aubry*, a professional photographer had taken a photograph of a young woman sitting on some steps in a public place. The photograph was used, without her consent, to illustrate an article in a literary magazine. The courts at all levels found that the photograph was in no way derogatory or humiliating to the individual *per se*, neither in the way the individual was portrayed, nor in any relationship that it had to the text. Damages of C$2,000 were awarded at trial. In the Supreme Court the issue was whether there had been sufficient evidence of humiliation damages arising out of the invasion of privacy in order to support the action in tort. There was dissent, and although the award of damages was considered high, the award was upheld. The only evidence of damages was that the young woman had

---

[53] [1991] R.R.A. 421 (Cour du Québec); (1996), 71 C.P.R. (3d) 59 (Que. C.A.); [1998] 1 S.C.R. 591. (S.C.C.).

testified that she had some difficulties at school because her friends teased her.

(b) Other Common Law Remedies

To generally assist the development of a common law tort of invasion of privacy, four of the ten Canadian provinces[54] have passed legislation simply providing that it is "...a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of an individual". However, these statutes have been rarely used. One of the reasons for this may be that in each province actions for invasion of privacy must be brought in the superior trial court of the province, which requires significant initial expenditure by the complainant.[55] On the other hand, damages in privacy actions are uncertain. Damages are dependent on the facts in each particular case, and precise calculations in advance may be impossible.

Some have argued that required use of the superior trial court is the reason for the general lack of use of the statutes. The cost of bringing an action in a superior court is often outweighed by the potential recovery of any damages.

(c) Class Actions

As a solution to problems of costs in litigation in general, class action proceedings are now permitted in all Canadian provinces, either explicitly by statute, or implicitly by reason of the decision of the Supreme Court of Canada in *Western Canadian Shopping Centres.*[56] The widely accepted goals of class actions are to promote judicial economy, to make the court system more accessible to the public, and to modify the behaviour of potential defendants. It is likely that a court would see a claim based on non-

---

[54] British Columbia in 1968, see the *Privacy Act*, R.S.B.C. 1979, c.336; Manitoba in 1970, see *The Privacy Act*, R.S.M. 1970, c.74; Saskatchewan in 1974, see *The Privacy Act*, R.S.S.1978, c.P.24; and Newfoundland in 1981, see the *Privacy Act*, R.S.N. 1990, c.P-22. These were based in part on Sections 50 and 51 of the New York Civil Rights Law.

[55] See G.H.L. Fridman, *The Law of Torts in Canada, Volume 2* (Toronto: Carswell, 1990) at 200-201; and Burns, "The Law and Privacy: The Canadian Experience" (1976), 54 C.B.R. 1 at 38.

[56] *Western Canadian Shopping Centres v. Dutton*, [2001] 2 S.C.R. 534.

compliance by a large organization with a privacy law such as PIPEDA as a very appropriate use of the class action proceedings.

Notwithstanding the passing of legislation to permit class actions, it has taken time to develop a bar experienced in the financing and prosecuting of these types of actions.[57] Canada's first privacy class action was filed in Regina, Saskatchewan on February 3, 2003[58] under that province's class action law that came into force January 1, 2002.[59] Insofar as is known, it did not rely on PIPEDA as a basis for liability, and Saskatchewan does not have a private sector privacy law of general application. It arose out of the loss of a hard drive containing financial and account information on an estimated one million people, and it put each of them at a higher risk of identity theft.

Practice Note

Franchises that collect personal information that is likely to be targeted by identity thieves, such as credit card information for payment in e-commerce, will have a higher risk of liability and therefore should implement strong security procedures. The computers that hold such customer details must be always accounted for and guarded.

Claims arising only out of the improper collection and use of customer information may present greater challenges in estimating damages because of the difficulty in calculating damages for humiliation, but in the United States such actions have proven to be an effective enforcement tool.

(d) Actions for Misrepresentation under the Competition Act

Further liability can arise out of the privacy statement required under PIPEDA or other privacy law if the statement does not accurately reflect the privacy policies of the organization. Such a situation has been the basis for many class action proceedings for the breach of privacy rights in the United States.

---

[57] See Peter Bakogeorge, " Making a class-action plan", *Law Times*, September 10, 2001, at p. 15.
[58] Richard Foot, "Class action says firm 'negligent' in data loss", *National Post*, February 4, 2003.
[59] *The Class Actions Act*, Ch. S.S. 2001, c. C-12.01.

Section 52(1) of the *Competition Act*[60] provides as follows:

> No person shall, for the purpose of promoting, directly or indirectly, the supply or use of a product or for the purpose of promoting, directly or indirectly, any business interest, by any means whatever, knowingly or recklessly make a representation to the public that is false or misleading in a material respect.

This provision is in the criminal offence section of the *Competition Act*. There is a similar provision in section 74.01 in the reviewable matters portion of the *Competition Act*. The difference is that the criminal offence requires that the misrepresentation be made knowingly or recklessly.

If a court finds that an organization has breached section 52(1), being the criminal offence under the *Competition Act*, there is a private right of action under Section 36(1) of the *Competition Act* for damages proved to have been suffered and caused. In the past, this private right of action for damages has not been widely used. Some feel that this is because that damages alone in many competition law matters are not significant enough to offset the costs of bringing the action. These actions may be brought in any court of competent jurisdiction, and thus as a class action bar develops there has been an increase recently in the number of class proceedings that are being brought in provincial courts in reliance upon this section. However, in a privacy based misrepresentation case, the number of defendants may be very significant, making a class action economically viable even if the estimate of individual damages is relatively low.

In addition to the action for misrepresentation under the *Competition Act*, there may also be an action for fraudulent misrepresentation based in contract law.

(e) Remedies and Enforcement: Summary

Currently almost all reported privacy disputes have been dealt with as complaints to the Privacy Commissioner of Canada or the Commission d'accès à l'information du Québec. No decisions have been released by the privacy commissioner in British Columbia and only one decision has been released in Alberta. And few of the decisions of the Privacy Commissioner of Canada have been considered by the Federal Court.

---

[60] R.S.C. 1985, c. C-34, s.1.1.

Certainly, at this time, the remedies for a breach of PIPEDA or one of Canada's other privacy law are not particularly onerous. At present, most privacy commissioners are sensitive to the challenges of complying with a new law. But based on the review of remedies discussed above, franchisors should be aware when designing business models and systems that this situation may change. On the other hand there may also be time to adapt.

IV. Specific Implications For Franchisors

Privacy laws have little effect on franchisors *per se*. Their primary effect on franchisors and the franchise systems arises out of their effect on marketing and customer relationship issues. Prior to the passage of privacy laws, customer information could be collected, used and exchanged between franchisees and franchisors almost without restriction. Now all such activities in Canada must have the consent, either explicit or implied, of the individual customers. The nature of the form of consent used must take into account the "sensitivity" of the personal information, and thus certain sectors, such as child care and financial services, will be affected much differently than vendors of hamburgers and pizza.

The franchisee application forms of all franchisors will have to be revised to take into account Canada's new privacy laws, and in particular the notice provisions of section 4.8.2 of the Schedule to PIPEDA.[61] Franchise systems that require stores with video or other surveillance may unintentionally find themselves involved in significant privacy disputes between their customers. And consent can only be obtained for identified purposes. Some retail sectors are having difficulty training staff to effectively communicate the purposes for the collection and use of personal information.

A. IMPLICATIONS OF THE CONSENT REQUIREMENT

Manufacturers and franchisors may no longer simply require by contract that their dealers and franchisees turn over customer information in order to build a customer database and ensure ownership of the customer list. Now the franchisee must obtain the consent of the customer not only to collect and

---

[61] In a personal communication the Privacy Commissioner of Canada verbally advised the writer that she would not hesitate to investigate a complaint from a prospective franchisee whose personal information was collected by an American franchisor with no other operations in Canada, notwithstanding the jurisdictional questions.

use the information, but also obtain consent for any required disclosure to the franchisor, and consent for the franchisor's proposed uses of the information. While consent to the collection and use of such information in a store may often be implied from the actions of the customers, the same cannot always be said for the disclosure to the franchisor. Further customers cannot be required to provide personal information beyond that "...required to fulfill the explicitly specified, and legitimate purposes..." of a transaction.[62]

Insofar as the marketing programs are administered centrally by the franchisor, they will be affected by the new consent requirement. Examples include marketing surveys, warranty programs, direct mailings, contests and games, data mining, and customer support.

Consent in the privacy context is very much like the concept of consent with respect to the formation of contracts. There must be a meeting of the minds with respect to how the personal information will be collected, used or disclosed. In many commercial contexts, such consent or agreement is evidenced by comprehensive written documents. Problems arise in commercial transactions that are routine and where the individual parties have significantly different values ascribed to the outcomes, such as, for example, a small supplier to a large automobile manufacturer.

Consumer transactions generally involve a larger proportion of less sophisticated and more vulnerable individuals than commercial transactions. Generally, the ability of the vendor to come to a meeting of the minds with the consumer using long and complex written terms and conditions is limited not only by the inability of any set of terms and conditions to fully foresee future developments, but also by the ability and/or willingness of the consumer to absorb all the complexities of the vendor's offer. In contract law these problems have led to judges trying to intervene on grounds such as unconscionability, fiduciary duty or good faith to correct perceived unfairness in the formation of these contracts.

While obtaining consent under privacy laws has many of the same problems as in the formation of consumer contracts, the parameters of the variables and policy concerns are still being developed in this relatively new area of law. This, and perhaps the inherent nature of the concept of privacy, have led to concerns that privacy laws are very vague. Businesses feel frustrated when their lawyers cannot give them clear black and white answers as to whether or not a particular practice complies with the law.

---

[62] *Supra* note 22 at Paragraph 4.3.3 of Schedule 1.

This was one of Ontario's criticisms of PIPEDA that was given as a reason for the drafting of the Ontario privacy law that was never introduced in the Legislature.[63]

Such vagueness is not necessarily a bad thing. While businesses are concerned that some of their practices may fall into a grey area with respect to compliance, an individual is also less likely to commence a costly court action if the chances of winning are less certain. While the consumer may complain, the most appropriate and cost-effective dispute resolution procedure for both parties in these circumstances is negotiation and mediation. This is in fact what many Canadian privacy commissioners do.

The most significant variables to consider when obtaining consent under privacy laws are the sensitivity of the information, the purposes for which it will be used, and the security under which it will be held.

Practice Note

Assess the sensitivity of the personal information that a franchisor collects uses or discloses carefully when designing collection procedures and consent forms.

B. WHAT IS " SENSITIVE INFORMATION"?

The concept of "sensitive information" is important for determining the appropriate form of consent to be obtained, and the nature of the security to be used to protect personal information. Obtaining the appropriate form of consent, either explicit or implicit, is the key to compliance with PIPEDA. If the consent is defective, then all uses of the personal information, whether it is properly protected or not, are a breach of the legislation. Further, security measures are among the more expensive requirements of compliance with PIPEDA. The choice of inappropriate provisions may lead to costly upgrading.

The concept of "sensitive information" is not defined in PIPEDA. However paragraph 4.3.4 of Schedule 1 to PIPEDA states that:

---

[63] Ontario Ministry of Consumer and Commercial Relations, *A Consultation Paper: Proposed Ontario Privacy Act* (Toronto: Ministry of Consumer and Commercial Relations, July 2000).

> Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context.

The next paragraph goes on to specify that the "reasonable expectations of the individual" are also relevant in obtaining consent. Concerns about the sensitivity of different types of information vary with the culture. Differences between the attitudes of Europeans and Americans to the role of government in their lives exacerbated the negotiations over the Safe Harbor proposal for American compliance with the E.U. Data Directive. While Europeans believe that government has a duty to protect the privacy of its citizens, they find questions regarding political affiliation or ethnicity objectionable. Americans answer these questions regularly, but are sensitive about financial disclosure and have an inherent distrust of government's ability to protect their rights.[64]

Other jurisdictions have specified certain types of information as being generally "sensitive", and built in protections, such as requirements for explicit consent or special handling. For example, the United Kingdom's *Data Protection Act, 1998*[65] in section 2 defines "sensitive personal data" to mean personal data consisting of information as to:

> (a) the racial or ethnic origin of the data subject;
>
> (b) his political opinions;
>
> (c) his religious beliefs or other beliefs of a similar nature;
>
> (d) whether he is a member of a trade union (within the meaning of the *Trade Union and Labour Relations Consolidation Act 1992*[66]);
>
> (e) his physical or mental health or condition;
>
> (f) his sexual life;

---

[64] Europeans and Americans have divergent ideas on government protection and corporate responsibility. "There are some profound differences between the two populations," Dan Griswold, associate director at the Center for Trade Policy Studies at the Cato Institute, Washington DC, as quoted in Scott Miller, "U.S.-EU Summit Will Address Trade Tensions" *Wall Street Journal Online*, June 24, 2004.

[65] (U.K.), 1998, c. 29.

[66] (U.K.), 1992, c. 52.

(g) the commission or alleged commission by him of any offence; or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Section 4 of the *Data Protection Act, 1998*, also refers to data protection principles that are set out in schedules. Schedule 3 applies only to sensitive personal data and requires that the data subject has given explicit consent to the processing of such data.

Australia has a similar list of prescribed types of sensitive information that also includes information about the individual's "...lifestyle, character or reputation."[67] Organizations are prohibited from collecting such information unless they obtain consent. However, there is an exemption for non-profit organizations that have only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims. These organizations may collect sensitive information about their members or other individuals with which they have regular contact if, prior to collecting the information the organization undertakes to the individual that the information will not be disclosed without the individual's consent.

In the Spanish *Ley Orgánica 15/1999*[68] Article 7 sets out what is "specially protected" data. In this statute, the list is first divided according to those items, such as ideology, religion or beliefs, which are protected under the Constitution. These require the highest level of explicit consent. There is then a further category which includes data that will reveal the ideology, union affiliation, religion or beliefs, for which there are certain exceptions for the maintenance of lists by unions political parties, churches and other such groups. Personal information having reference to racial origin, health and sexual life can only be collected when for reasons of public policy, it is made possible by a law or by express consent. Finally, it is prohibited to create data files for the exclusive purpose of revealing the ideology, union affiliation, religion, beliefs, racial or ethnic origin or sexual life of an individual.

Similarly, the French *Loi No. 78-17 du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés* in Article 31 prohibits maintenance of data files that will reveal racial origins, religious,

---

[67] *Privacy Amendment (Private Sector) Act 2000*, Act No. 155 of 2000, which came into force on December 21, 2001.

[68] *Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal.*

philosophical or political opinions or union affiliations, or "... les moeurs ..." of individuals without the express agreement of the individual. However, the maintenance of membership lists by groups such as churches, political parties and unions is specifically allowed.

Section 28 of Germany's *Bundesdatenschutzgesetz*[69] sets out certain conditions for the storage, communication and use of data for an organization's own purposes. Previously some protection was given to sensitive personal information such as health matters, criminal offences, administrative offences, religious or political views and trade union status. Effective May 23, 2001 the *Bundesdatenschutzgesetz* was amended to include all of the categories of sensitive information contained in Article 8 of the E.U. Data Directive.[70] Now the collection of such data must be expressly approved by the data subject, and its processing requires a prior review by a data protection official.

From this simple survey, it is clear that many democratic countries regard information about an individual's religious, political or philosophical beliefs as being sensitive, and restrict its collection, use and disclosure.

Similar generally sensitive areas may be inferred in Canada from an examination of those rights and values that are specifically protected by law. If such rights and values have been given special protection, the collection of information about the exercise of that right or expression of that value may inhibit the exercise of the right or the expression of the value. Accordingly, the information may be considered "sensitive" as that term is used in PIPEDA. For example, to safeguard the freedom to vote according to one's own belief or conscience[71] Canada uses secret ballots. Privacy or secrecy is considered key to the protection of the right to vote according to one's own conscience. The collection information on how people actually voted may be considered sensitive and require consent.

Section 2 of the *Canadian Charter of Rights and Freedoms*[72] (the "*Charter*") provides a list of fundamental freedoms:

(a) freedom of conscience and religion;

---

[69] Vom 20.12.1990, BGBI. I S. 2594.
[70] *Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze*, BGBI vom 22.05.2001 S.904.
[71] As expressed in Sec. 3 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act*, 1982 (U.K.), 1982, c.11.
[72] *Ibid.*

(b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;

(c) freedom of peaceful assembly; and

(d) freedom of association.

Further, section 15(1) provides that every individual is equal before and under the law, without discrimination, including discrimination based on: race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.

Any collection, use or disclosure of personal information dealing with these characteristics will most likely be regarded as sensitive, because if the information is used for the wrong purposes, such use would most likely violate the freedoms or rights that the individual has under the *Charter*.

Not all the rights provided in the *Charter* will be equally sensitive. It is posited that "sensitivity" will be based on the abilities of others to use such information to take any action harmful to the interests of the individual. For example, usually the sex of a person can be determined by simple observation, or inferred from the name. Therefore, a list of names identifying such persons as male or female may not be considered particularly sensitive.

However, a list of the names and addresses of the attendees at a local synagogue or mosque, or of the members of the Catholic Church that are also active in Campaign Life, would most likely be considered much more sensitive.

On the other hand, some areas that are considered sensitive by many in North America are not considered sensitive in Europe, and have not been included in the *Charter*. The most prominent example is financial information. In contrast to Europe, in the United States the financial services sector was one of the first areas to be the subject of a sector specific law.

Other concerns may arise only if the information is transferred out of the jurisdiction. In British Columbia, a union was concerned about outsourcing and obtained an opinion from a lawyer with the American Civil Liberties Union regarding the implications of the *Patriot Act*[73] on information outsourced to a U.S. business for processing. The primary concern was that

---

[73] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, Public Law 107-56.

such information could be accessed by the U.S. government without the consent or knowledge of the individuals involved. The Office of the Information and Privacy Commissioner for British Columbia is now conducting an assessment of these concerns.[74] In the meantime, individuals in British Columbia are raising concerns regarding other cross-border transfers of personal information in other contexts.

Accordingly, franchisors in areas such as personal health, education, financial services, child care and senior care may find that Canada's new privacy laws will have significant impact on their methods of customer relationship management.

C. COMMUNICATION OF PURPOSES

The communication to the customer of the purposes for which the personal information is collected, used or disclosed is an essential requirement in obtaining consent. For example, British Columbia's *Personal Information Protection Act* ("PIPA") requires that:

> 10 (1) On or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing:
>
> (a) the purposed for the collection for the information; and

---

[74] Office of the Information and Privacy Commissioner for British Columbia, Request for Submissions: Assessing USA Patriot Act Implications for Privacy Compliance under British Columbia's Freedom of Information and Protection of Privacy Act, May 28, 2004. Available on the web site of the B.C. Commissioner, <http://www.oipc.bc.ca>. On July 23, 2004 the Government of British Columbia made public its submission to the Information and Privacy Commissioner and announced that it would be amending the *Freedom of Information and Protection of Privacy Act* to apply privacy standards directly to third party service providers in outsourcing situations, and to require notice to the government of requests from foreign bodies for production of information. See Government of British Columbia, Submission to the Information and Privacy Commissioner for British Columbia: Examination of USA PATRIOT ACT implications for personal information of British Columbia residents involved in outsourcing of government services to U.S.-linked service providers, (Victoria, B.C.: Government of British Columbia, July 23, 2004).

(b) on request by the individual, the position, name or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about collection.

Sometimes the communication of the purposes can be delicate. It is common practice in retailing to collect personal identifiers from persons returning goods for purposes of loss and fraud prevention. But advising a customer that the store insists on knowing certain personal information because it is concerned that the customer might be a thief is not easy, and it is not a task easily delegated to young, mobile and distracted retail clerks.

Since the coming into full force of PIPEDA on January 1, 2004, the Office of the Privacy Commissioner of the Canada has received numerous complaints about the returns practices of retailers in Canada. After a meeting with the Retail Council of Canada, a spokesperson for the Office announced that retailers will have to work harder at communicating purposes to customers. Generally this will mean the preparation of information pieces that can be distributed to customers seeking further information regarding purposes for the collection of their personal information.

D. PREMISES AND SECURITY

Where the franchisees operate a significant retail space, such as a store, it is very common to have various forms of surveillance and security to protect the premises and the inventory, most commonly video surveillance. Under Canada's privacy laws the consent of the customer is needed to collect and store the surveillance information.

This is not difficult to accomplish. Signs at the entrances to the premises should announce the presence of such surveillance, and its purposes. Reference should also be made to the fact the information collected will be retained. Customers walking in and shopping after having had a reasonable opportunity to view the signs are deemed to have consented to the collection and use of the information for security purposes.

More significant problems have arisen where conflicts have arisen between customers, such as couples included in a custody fight, and the video-camera has dutifully recorded all the details. Acceding to the wishes of either party in the dispute with respect to the disclosure of the information collected may breach the other's privacy, and the other party may be strongly motivated to enforce their privacy rights. In circumstances such as these the retailers or franchisee will most likely have to incur the cost of sophisticated legal advice.

E. ACCESS BY INDIVIDUALS

Aside from particularly difficult access requests as described above, franchise systems will have to take into account the possibility of customer access requests when designing compliance systems. Principle 9 of Schedule 1 to PIPEDA states that 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. Paragraph 4.9.3 goes on to require that in advising as to which third parties a customer's information has been disclosed, organizations should be as specific as possible. Section 23 of British Columbia's PIPA requires the disclosure of the names of individuals and organizations to which the personal information has been disclosed.

One of the lessons learned from Québec with respect to access is the importance of having a file system for the storage of personal information that provides easy access to all files relating to a particular customer, yet allows for segregated sub files for more sensitive matters. In retailing or e-commerce, this means that customer information should be separated into basic demographic information, such as name and address, which are not particularly sensitive; and the credit card and billing information which are sensitive, and which cannot be retained as long as demographic information. If the franchise system decides to function as a single organization in matters of privacy compliance, such filing system will have to be implemented uniformly by franchisees.

Practice Note

If a significant volume of access requests are anticipated, be sure that files for different matters for the same individual are linked.

V. Compliance Options

As noted earlier, privacy laws have little effect on franchisors *per se.* Their primary effect on franchisors and franchise systems arises out of their effect on marketing and customer relationship issues. In this section basic compliance advice is provided first, followed by a discussion of issues specific to franchisors.

A. BASIC PRIVACY COMPLIANCE STEPS

The basic steps for complying with a privacy law are common to all organizations, and a guide to such steps is set out below.

1. Appoint a Compliance Officer

The first step is to put someone in charge of the process, or at least to choose a co-ordinator, and have that person be the compliance officer required by Principle 1 of the Schedule to PIPEDA.[75] The individual should obtain copies of the relevant legislation and regulations, and knowledgeable legal and other support. The individual may then assemble a team to oversee and/or conduct the audit and implementation steps that will be described in the next sections. The Compliance Officer and her team should then develop a draft plan to implement policies and practices to comply with the relevant privacy laws after the conduct of the audit.

The plan should address:

1. implementing procedures to protect personal information;
2. establishing procedures to receive and respond to complaints and enquiries;
3. training staff and communicating to staff information about the organization's policies and practices;
4. developing information and explaining the organization's policies and procedures; and
5. ensuring the accuracy of the personal information held by the organization and updating any retention policies.

2. Conduct a Privacy Audit

The purpose of the audit is to establish what personal information is currently being collected, used or held, or disclosed by the organization, and how is it currently stored and protected.

The audit should also identify all jurisdictions where personal information is being collected, as it may be necessary to comply with other privacy laws. For commercial organizations, privacy issues arise in the following areas:

- marketing and sales
- human resources
- online operations (items such as computer cookies)
- government relations (lobbying)
- client or customer files

---

[75] See also s. 4(3) of B.C.'s PIPA; s. 5(3) of Alberta's PIPA.

- security services

Particular care should be taken to identify personal information that is disclosed to subcontractors such as: employee information to payroll services, marketing information to ad agencies, information submitted on-line to service fulfilment providers or data analysers, lobbying information to trade associations, and mailing information to outside mailing firms. Copies of the contracts with each subcontractor should be reviewed with respect to privacy protection.

3. Develop a List of Approved Purposes

After having conducted the audit, the organization should then examine the purposes for which it is collected, and the nature of the information collected, to determine the organization's long term policy as to purposes and the types of information that are truly necessary to fulfill those purposes. Many organizations have discovered that they are collecting more information than is reasonably necessary.

This information will not only become the basis for the drafting of the official privacy policies and guidelines, but also the various consent forms that will be used, or other methods of collection.

In Québec such purposes or "objects" are required to be kept in individual's file. Under PIPEDA, if new purposes are added in the future, additional consents must be obtained.

4. Prepare Privacy Policies, Brochures and Consent Forms

Having made decisions about the overall purposes for which the organization will collect personal information, the next step is to implement the decision by preparing the organization's privacy policies and guidelines. The privacy brochures mentioned in paragraph 4.8.2. of the Schedule to PIPEDA must also be prepared, as well as the privacy statements necessary to comply with PIPEDA. The preparation of consent forms or other collection methods will require decisions as to the nature of the consent and disclosure required based on the sensitivity of the personal information being collected. Will explicit or implicit consent be used? How will the privacy policy be positioned on the home page of your website? Will "click-through" consent be required?

5. Consider a New Filing System

Experience in jurisdictions with privacy laws, such as Québec, has shown that one of the keys to low cost compliance with access requests is having a filing system that segregates personal information with respect to each individual according to the purpose for which the information was collected, yet has links and controls on the setting up of new files with respect to any individual. If files are computerized, this generally means that the databases in membership and other areas should be linked. Experience recently in the United States with respect to the *Gramm-Leach-Bliley Act*[76] has suggested that where this linking is not done, or cannot be done, compliance will be lower and costs will be higher.

Not all purposes require the collection of equally sensitive personal information, and if all information regarding an individual is in one file, then that file must have safeguards appropriate to the most sensitive aspect of the file. If an access request is made, and there are grounds for denying access to one portion of the file, then the file will have to be reviewed item by item to determine what must be severed, and what may be disclosed to the individual.

6. Initiate the Privacy Plan

Obviously the decisions mentioned earlier will have to be implemented. The implementation is often co-ordinated so that the organization is comfortable that from a certain date forward, the organization generally complies with the privacy requirements. It is also necessary to review existing files containing personal information and to either ensure that there is appropriate consent for the retention and use of the information, or that the information is safely deleted. This may require a mailing or other communication with the individuals to announce and explain the new privacy policy and obtain the new consent.

Implementation may also require changes to any websites that the organization has to ensure, among other things, that persons using the website have access to a copy of the privacy policy or statement every time personal information is submitted. At this point the required safeguards for the personal information should be in place, whether physical, technological or in staff policies regarding employee access. The policy regarding the

---

[76] *Supra* note 10.

handling of complaints should be ready, as well as the policy on whether to charge any amount to individuals requesting access. Contracts with subcontractors should clearly spell out the compliance measures necessary on their part, and provide the organization with a right of audit.

7. Maintaining Compliance

Set out below are some of the things to be considered after implementation to maintain compliance with PIPEDA and other privacy standards:

- Policies should be developed to ensure that evidence and documentation exists for:
  - each individual's consent, for each database and purpose;
  - all uses of, or disclosures from, each database are properly recorded and protected, and are in accordance with the purposes; and
  - review of the databases for accuracy in accordance with the sensitivity of the information.
- Responsibility for compliance may be better separated from responsibility for collection, use and disclosure. Collecting, use, and disclosure should not be able to proceed without authorization from the compliance officer.
- Provisions should be made for the regular training of new staff, and for review and update of the policies.
- The development and application of provincial laws should be monitored.
- Transactions with persons outside Canada should be monitored for potential breaches of foreign privacy laws.
- A response plan in the event of allegations of a privacy breach should be developed.
- Provisions should be made for internal or external compliance audits.

B. COMPLIANCE ISSUES FOR FRANCHISORS

The most fundamental decision to be made by a franchisor in implementing a privacy compliance program is the decision about the breadth of the program. Will there be one privacy policy and compliance program for the franchise system (that includes franchisees) or will the franchisor's privacy policy and compliance program be mandatory only for the franchisor, and franchisees will only be required to comply with the relevant privacy laws?

If the privacy policy is system wide, will it be for customers only, or also for employees?

In making these choices, the franchisor will have to take into account the degree to which privacy is relevant to the customer satisfaction associated with brand, and the risk of the assumption of liability for non-compliance with the privacy policy by a franchisee. If a privacy policy is system wide, who will respond in the event of a complaint, and how will the costs of a defence be allocated? These issues would preferably be worked out in advance.

As a formula for a franchisor wishing to undertake such an analysis, the process might be described as balancing (a) the marketing benefits likely to be derived from having a uniform system wide policy; against (b) the costs associated with implementing and policing a system wide policy; and (c) the risks of liability for franchisee conduct (vicarious liability) arising out of a system wide policy.

For example, a financial services franchisor may consider that concerns about client privacy are a very real part of the services being offered, and accordingly there are significant marketing benefits that might arise from a prominent and uniform approach. Implementation may not be as costly as some other sectors because financial professionals already conform to practices that ensure the confidentiality of client information. For the same reason, the increased risk of liability may not be significant.

On the other hand, generally little or no customer information is collected in the sale of hamburgers, and customer privacy is not generally considered part of the service. There would be considerable training costs to introducing privacy concepts and concerns to the franchisee's frontline staff. This would appear to be a system where the franchisor would be better off simply requiring franchisees to comply with all privacy laws.

But consider the marketing used by pizza chains. Orders are generally made by telephone, and many pizza chains collect and maintain significant computerized databases regarding their customer's preferences and the frequency of purchases. Consent is now required to continue this practice. On the other hand, many individuals do not consider their preferences in pizza to be particularly sensitive personal information, and thus it may be possible to use implied consent to continue the marketing practices. However, if the franchisees accept payment by credit card over the telephone, there are significant possible security and identity theft issues. How long is the card information retained? Is it adequately secured from theft? What is adequate security in the context of a pizza take-out store operated by teenagers?

As has been noted earlier, the primary branding issue to be taken into account is the degree to which customers considered a certain level of privacy protection to be part of the image associated with the brand. However, such associations may also be important for employee relations, if part of the branding image is that a franchisor is a progressive employer. Particularly relevant to the branding image will be clear communication as to the purposes for the collection, use or disclosure of personal information. As noted above, this has already proven to be a problem in some retail sectors.

Balanced against any benefits to be gained by having a uniform privacy policy are the costs of ensuring that the privacy policy is implemented uniformly by the franchisees, and the associated liabilities to the system and the brand associated with non-compliant individuals. Another liability concern will be the franchisor's liability to franchisees for advice on how to comply that is later determined to be inappropriate by a privacy commissioner. As was noted earlier, privacy law is new to Canada, and issues in Canada, and in fact much of the world, are still being worked out. Accordingly, there is a distinct possibility that despite best efforts on the part of the franchisor and its advisors, some issues in a privacy policy may be challenged by a customer and/or a privacy commissioner.

As was discussed earlier in the section on remedies, most challenges, while embarrassing, may not result in significant financial liabilities. But security issues have the potential to result in significant class action law suits. There has already been one class action filed in Canada resulting from the theft of a hard drive containing names, address and financial information on approximately one million Canadians. Payment information, such as credit card numbers, is particularly vulnerable to identify theft and abuse. These factors should be taken into account when designing any system wide file structure and privacy policy. Depending on the magnitude of these liability issues, it may be necessary to disclosure such issues in the disclosure documents required in Ontario and Alberta, and potentially in Québec.

Even if the franchisor decides not to implement a system wide franchise policy, it may wish to provide its franchisees with support in developing their own compliance strategies. Obviously to lessen the risk of liability, the franchisor will wish to ensure that any such support documents carry clear disclaimers and warnings regarding the responsibility of the franchisees to develop their own compliance program. Such support options include creating a separate "franchisee" privacy policy and requiring compliance with it; supplying the franchisees with the franchisor's privacy policy and

requiring compliance; or requiring the franchisees to submit their privacy policies for franchisor approval.[77]

Some factors that may tip the balance in favour of a system wide policy are the development of e-commerce by the franchisor and/or the development of uniform franchisee web-sites, particularly on an international basis. Obviously web-sites present greater opportunity for profiling customers. However, electronic payment options also increase the need for uniform security standards. If the franchisor is also operating in Europe or parts of South America, a high standard of compliance will be required. European privacy laws require notification to data protection agencies in advance, failing which there are significant civil penalties and possibly even criminal penalties. Enforcement of these laws is increasing. Generally, organizations have found that once a significant part of their operations are required to comply with a certain privacy standard, it may be cost effective to implement such standard across the organization.

VI. Conclusion

Privacy laws are not designed to affect franchise systems in particular. Rather they will primarily affect how franchisors design the marketing and employee aspects of their systems. In these areas, retailers and franchisors alike are still discovering the full implications of both Canada's new privacy laws, and the implications of having Canadian customers who are slowly and vaguely becoming aware of their new privacy rights.

To ensure continuing compliance, franchisors will have to monitor developments and emerging issues in this area on a regular basis and be prepared to modify their policies as changes occur.

---

[77] For a discussion of these support options, see Andraya C. Frith and Megan Hill, "PIPEDA for Franchise Lawyers" *The Lawyers Weekly*, June 25, 2004.