



*New Canadian Privacy  
Legislation Applies to All  
Franchises in Canada*

*Published in International Journal of Franchising Law, 2004, Volume 2, Issue 5, p.31*

*John L. Rogers*

*Chris L. Bennett*

2800 Park Place  
666 Burrard Street  
Vancouver, BC  
Canada V6C 2Z7  
Tel: 604.687.9444  
Fax: 604.687.1612  
[www.davis.ca](http://www.davis.ca)

© Davis & Company, 2005. This paper is the property of Davis & Company. No reproduction of any part of this paper is permitted without the prior permission of the authors.

This paper is intended to provide general comments on developments in the law. It is not intended to be a comprehensive review nor is it intended to provide legal advice. Readers should not act on information in the paper without seeking specific advice on the particular matter. Our firm would be pleased to provide additional details or discuss how this information is relevant to a specific situation.

# New Canadian Privacy Legislation Applies to All Franchises in Canada

*by John L. Rogers and Christopher L. Bennett*

*Davis & Company, Franchise Lawyers, Vancouver, British Columbia*

October, 2004

In this feature, John L. Rogers and Christopher L. Bennett explain the implications of the Personal Information Protection and Electronic Documents Act, which came into force in Canada earlier this year. This important legislation meets the privacy standards required by the European Union's Community Data Protection Directive, and needs to be complied with by all businesses operating in Canada, including franchise systems.

## **1. Background**

Privacy legislation is not new to Canada. The Federal Government and most provincial governments in Canada have been required to comply with public-sector privacy legislation for decades. However, until recently most private-sector organisations have not been subject to a comprehensive privacy protection regime.

This changed in 2000 when the Federal Government passed the Personal Information Protection and Electronic Documents Act ("PIPEDA"). Initially PIPEDA only applied to federally-regulated private sector organisations such as banks, airlines, and internet service providers. From January 1, 2004, PIPEDA (or substantially similar provincial legislation) applies to all businesses operating in Canada, including franchise systems.

PIPEDA meets the privacy standards required by the European Union's Community Data Protection Directive (94/46/EC). In fact, Canada's PIPEDA is the first non-European legislation to receive the European Commission's approval in this regard. Such approval allows personal information to continue flowing between the EU and Canada.

## **2. Scope of PIPEDA**

PIPEDA protects all “personal information” collected, used and disclosed during the course of commercial activities. “Personal information” includes information about a person’s race, age, marital status, religion, employment history, income, address, telephone number, email address, biological information and opinions.

Franchisors routinely collect personal information from their employees and franchisees. Likewise, franchisees routinely collect personal information from their employees and customers. PIPEDA and some provincial legislation contain strict rules regarding how this information may be collected, used, stored and disclosed.<sup>1</sup>

## **3. The Rules**

PIPEDA imposes significant obligations on franchisors and franchisees. For example:

### *3.1 Designate a Privacy Compliance Person*

Every franchisor must designate a person who will be accountable for privacy issues related to their employees, franchisees, suppliers and customers. The privacy officer will educate staff and manage inquiries and complaints.

### *3.2 Identify Purposes*

Franchisors must explain to each individual why and how they wish to collect and use that individual’s personal information. They must also explain why, how and to whom they may wish to disclose such information.

### *3.3 Obtain Informed Consent*

Franchisors must obtain an individual’s informed consent before collecting, using or disclosing any personal information about the individual. The consent may be explicit or implied, but it must have been given freely. Written consent is preferable, but not mandatory.

### *3.4 Limit Collection, Use and Disclosure*

Franchisors must not collect, use or disclose more information than is reasonably necessary under the circumstances. And they must not collect, use or disclose information for any purpose unless the individual involved has consented to that purpose.

### *3.5 Destroy Information*

Franchisors must destroy personal information once it is no longer needed for the purposes for which it was collected.

### *3.6 Ensure Accuracy*

Franchisors must keep their personal information records accurate and complete. And they must allow individuals to challenge the accuracy of their personal information and have inaccuracies corrected.

### *3.7 Provide Access*

Franchisors must tell individuals about the existence, use and disclosure of their personal information. They must also give individuals access to that information, with some limited exceptions.

### *3.8 Secure Information*

Franchisors must protect personal information from unauthorised access and disclosure. The required level of protection varies with the sensitivity of the information. Financial and health information are considered extremely sensitive.

### *3.9 Explain policies*

Franchisors must explain their privacy policies and procedures upon request.

### *3.10 Provide Recourse*

Franchisors must implement procedures to receive and respond to complaints and inquiries. Not only is this required by the legislation, but it is also a good way for franchisors to prevent problems from escalating to the privacy commissioners or the courts.

## **4. Franchisees**

Franchisees have the same duties as franchisors with respect to their own employees and customers. Furthermore, when customer information is exchanged between franchisee and franchisor, the franchisee must have obtained consent from the customer to disclose the information to the franchisor, and the franchisor must have obtained consent from the customer to collect the information from the franchisee.

## **5. Exceptions**

There are some exceptions to the above rules. For example, consent is not needed to collect personal information solely for journalistic, artistic or literary purposes. Nor is consent required when it is clearly in the individual's interests to collect the information and it is not possible to obtain consent in a timely way. Other limited exceptions may apply.

## **6. Remedies**

The legislation establishes a complaint procedure which empowers officials (known as "privacy commissioners") to investigate and audit a private organisation's information management practices. The legislation also gives the privacy commissioners the power of embarrassment, in that they may publicise the results of their investigations. Many of the Federal Privacy Commissioner's decisions to date have been reported in the Canadian media.

If a complaint is not resolved by a privacy commissioner, the legislation allows the dispute to be heard in court using "summary" proceedings. Courts are empowered to make a summary award of damages against anyone who breaches the legislation.

## **7. Impact of PIPEDA on Existing Databases**

There is no "grandfathering" provision in the legislation, so franchisors and franchisees will not be able to continue using previously-collected personal information if they do not obtain proper consent to on a going-forward basis.

## **8. Termination of Franchise Agreement**

A franchise agreement typically contains provisions describing what may or must happen when the agreement is terminated. Such provisions often require the franchisee to "de-identify" its operations by ceasing to use the franchisor's intellectual property and to return all confidential information (including the operations manual) to the franchisor.

The agreement may also require the franchisee to deliver customer lists and databases to the franchisor. However, without careful planning, this provision will contravene PIPEDA because the franchisor needs consent to collect the information from the franchisee. Likewise, the franchisee needs consent to disclose the information to the franchisor.

Accordingly, a franchisor should ensure that whenever its franchisees collect any personal information during the course of the franchise relationship, its employees, customers and potential employees and customers consent to their information being given to (and used or disclosed by) the franchisor at any time.

## 9. Compliance

The initial steps towards compliance should include:

- conducting internal information audits to determine when, how and why personal information is collected, how it is disclosed, where it is stored, and how it is protected;
- updating employment applications and contracts, franchise applications, franchise agreements, purchase orders, registration forms and other documents to include privacy disclosure and consent provisions in legal formats;
- obtaining written consent regarding information collected in the past and which may be collected in the future;
- appointing and training an internal privacy officer; and
- creating internal and external privacy and complaints policies.

Franchisors and franchisees should contact their Canadian legal advisors to begin working on a compliance strategy as soon as possible.

### ***John L. Rogers***

John L. Rogers is a partner of Davis & Company, a law firm established in 1892 with offices across Canada and in Japan; he chairs the firm's Franchise & Distribution Group. Mr. Rogers is a director of IFA's Supplier Forum.

### ***Christopher L. Bennett***

Christopher L. Bennett is an associate at Davis & Company and a member of the firm's Franchise & Distribution and Intellectual Property Law Groups.

(Footnotes)

<sup>1</sup> In general, PIPEDA does not protect personal information about employees of franchisors or franchisees; however, employees' personal information is protected by privacy legislation in some Canadian provinces.