JULY 2000
VOLUME NO. 4 ISSUE NO. 7

FEATURE

BILL C-6: A NEW PRIVACY PARADIGM

By Barbara McIsaac, Q.C., Rick Shields and Kris Klein, McCarthy Tetrault

The federal government's Bill C-6, known as the "Personal Information Protection and Electronic Documents Act" (the "Act") will usher in a new era of privacy legislation in Canada with potentially far ranging effects on the private sector. The Act will impose significant restrictions on the collection, use and disclosure of personal information across Canada. Although C-6 is perceived as having a high tech and e-commerce focus, it may ultimately affect every business in the country.

Background

C-6 is intended to respond to changes brought about by technological advances in the field of information exchange. It is an outgrowth of the "Canadian Electronic Commerce Strategy" announced by the Prime Minister in September 1998, which aimed to make Canada a world leader in electronic commerce before the end of 1999. C-6 deals with a number of distinct information-related issues that are linked by the theme of technological change.

As stated in section 3, Part 1 of C-6 seeks:

> "to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

Parts 2 through 5 establish the means for doing business with the federal government electronically, for submitting and proving electronic records in court and for the promulgation of federal government publications by electronic means. This legal update focuses on Part 1 of C-6, which we believe will have the greatest impact on Canadian business.

Part 1 represents, at least in part, the federal government's response to new privacy legislation in Europe. As a result of the European Union's ("EU's") issuance of the Directive on Data Protection in 1995, the member states of the EU have been obliged to pass data protection laws aimed at the private sector which are now, or soon will be, in force. Since a common feature of these laws is a restriction on the transmission of personal information to jurisdictions outside of the EU that lack comparable privacy safeguards, Canada risked interruptions in data flows between Europe and Canada if counterpart legislation was not put in place. Accordingly, C-6 represents Canada's somewhat grudging move away from a reliance upon industry self-regulation that has heretofore been an explicit facet of federal privacy policy. By initiating these changes, Canada is distancing itself from the privacy policy of the United States' federal government, which has so far resisted calls to adopt comprehensive private-sector privacy legislation.

Part 1 of C-6 is not directly modeled on the European laws. It explicitly incorporates and adopts, with some significant modifications, the Canadian Standard Association's *Model Code for the Protection of Personal Information* (the "Code") published in 1996, making compliance with the Code mandatory and adding a range of sub-

CANADIAN RISK AND INSURANCE MANAGEMENT SOCIETY ANNUAL CONVENTION
October 15-18, 2000 Edmonton, AB
Contact: (403) 750-3699.

INSURANCE BROKERS ASSOC. OF ONTARIO CONVENTION
October 18-20, 2000 Toronto, ON
Contact: (416) 488-7422.

RCCAQ ANNUAL MEETING
October 18-21, 2000 Quebec City, QC
Contact: (450) 674-6258.

ATLANTIC ALLIANCE CONVENTION
October 19-21, 2000 Halifax, N.S
Contact: Bruce Lipsett (902) 543-7222 or Rod Jones (902) 893-4204.

REGISTERED INSURANCE BROKERS OF ONTARIO ANNUAL MEETING
November 2, 20000 Toronto, ON
Contact: (416) 365-1900.

QUOTABLE QUOTE

Organizations will often not be aware of the many ways in which personal information that they collect ultimately gets used or disclosed. Furthermore, identifying publicly the purposes for which information is used or disclosed in order to comply with the requirements of C-6 will be a two-edged sword.

Bill C-6: A New Privacy Paradigm

Page 50

Canada is distancing itself from the privacy policy of the United States' federal government, which has so far resisted calls to adopt comprehensive private-sector privacy legislation.

stantial enforcement mechanisms.

The Code, appended as Schedule 1 to C-6, establishes ten principles for privacy protection:

- accountability of the party dealing with personal information;
- identifying purposes for collection, use or disclosure;
- consent to collection, use or disclosure of information;
- limiting collection;
- limiting use, retention and disclosure;
- ensuring accuracy;
- implementing safeguards;
- openness;
- individual access; and
- implementing procedures for challenging compliance.

The Code establishes that the personal information of an identifiable individual cannot be collected, used or disclosed without the individual's knowledge and consent except in limited circumstances. C-6 obliges organizations, in most cases, to obtain personal information directly from the affected individual and to inform that individual of the use to which the information will be put.

C-6 vests substantial powers in the Office of the Privacy Commissioner of Canada, an existing federal regulatory agency responsible for the enforcement of the federal Privacy Act. The Commissioner is authorized to receive complaints, conduct investigations and audits and make reports on his findings. The penalties for interfering with the Commissioner in the course of an investigation or audit may be substantial; C-6 provides for fines of up to $100,000. Complainants will also have recourse to the Federal Court of Canada, which can order a business to amend its information practices, to publish notices concerning the corrective measures that it has undertaken to achieve compliance with C-6 and to pay damages to a complainant, including damages for any "humiliation" suffered by the complainant.

C-6 may eventually apply to all personal information:

- which an organization collects, uses or discloses in the course of commercial activity; or
- of employees of every federally regulated work, undertaking or business that is collected, used or disclosed by the employer in respect of its operations.

For an initial three-year period, however, C-6 will apply primarily to organizations involved in such federally regulated sectors as telecommunications, broadcasting, aeronautics, interprovincial or international bus, truck or rail transport, maritime shipping and banking. During that period, Part I would not apply to an organization in respect of personal information that it collects, uses or discloses within a province whose legislature has the power to regulate the collection, use or disclosure of the information, unless the organization does it in connection with the operation of a federal work, undertaking or business or the organization discloses the

information outside the province for consideration. Three years after section 30 of C-6 comes into force, the ambit of C-6 would be extended to apply to all provincially-regulated businesses engaged in the collection, use or disclosure of personal information within provincial boundaries in the course of commercial activity, subject to the federal government's right to exempt organizations, classes of organizations, activities and classes of activities from compliance with Part 1 in those provinces that have passed comparable privacy legislation. To date, only the Province of Québec has passed comprehensive private-sector privacy legislation.

The Act also contains a transitional provision that renders it inapplicable to "personal health information" (as defined) for a period of one year from the Act coming into force. The interrelationship between this one-year exemption and the longer three-year exemption remains unclear at present.

Status of C-6

The Act received Royal Assent on April 4, 2000. The Industry Minister has indicated that the Act will come into force on January 1, 2001. Accordingly, the one-year exemption period for personal health information will expire on January 1, 2002 and the longer three-year exemption period will expire on January 1, 2004.

Compliance Strategies

As will have become clear, the basic principles of C-6 and the Code are directed toward restricting the collection and use of information about individuals and ensuring that individuals are aware of what information about them is being collected, how it is being used and that they have consented, in most circumstances, to both collection and use. Accordingly, the first step for most organizations, even before they can decide if they are subject to the provisions of C-6, will be to conduct an audit of their business to determine:

- What personal information do we collect?
- Why do we collect it?
- How do we collect it?
- What do we do with it?
- Where do we keep it?
- When is it used or disposed of?
- To whom is it given?
- Are we covered by this law?
- Can we avoid this law?

If your business is subject to C-6, you will need to address the following questions:

What Are We Talking About?

One of the questions that has led to some of the most difficult litigation pursuant to the federal *Privacy Act* is "what is personal information?". Interestingly enough, the definition of "personal information" in C- 6 reads as follows:

> ...Information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

By contrast, the federal Privacy Act contains a very extensive definition of personal information and is quite specific in some of those areas where there might otherwise have been differing views, e.g. "Are my views about you my information or your information?" Our expectation is, given the approach that the Courts have taken with respect to privacy in other contexts such as the criminal law, that the legal interpretation of the term "personal information" as it is used in C-6 may evolve to capture information in any form which can be tied to a specific individual.

Who's Going To Do It?

Your organization will be required to designate an individual who is both responsible for and accountable for its personal information handling practices. Depending on the size and nature of your organization, it may or may not already have individuals in place whose current job descriptions could easily encompass responsibility and accountability for compliance with the requirements of C-6. Insofar as C-6 addresses the privacy of employees and the protection of their personal information, the logical place to vest the authority and responsibility for personal information would be the Director of Human Resources. However, many organizations will also have personal information holdings that are captured by C-6 and are distinct from those related to their employees. A separate structure may be required in order to deal with responsibility for that information. In that case, a third or umbrella authority may be required in order to coordinate the activities of those responsible for employee information with those responsible for the other personal information. That coordinating role may well need to be a full-time one. At least in the initial stages, the person responsible will require ready access to counsel who are familiar with C-6 and can assist in the development of practices and procedures. Within that structure, your organization will also have to build in responsibility for dealing with requests for access to personal information both from employees and members of the public and the responsibility for dealing with complaints and interacting with the Office of the Privacy Commissioner if an investigation by the Commissioner is undertaken.

What Is Your Organization Doing With It Anyway?

One of the most difficult start-up issues for all organizations will be identifying the uses to which personal information is being put. Some uses will be easily identified. However, organizations will often not be aware of the many ways in which personal information that they collect ultimately gets used or disclosed. Furthermore, identifying publicly the purposes for which information is used or disclosed in order to comply with the requirements of C-6

C-6 obliges organizations, in most cases, to obtain personal information directly from the affected individual and to inform that individual of the use to which the information will be put.

will be a two-edged sword. Most organizations will want to define and publicize a broad range of uses in order to give themselves flexibility in the future. However, as the public becomes more aware of the law it may be counter-productive to advertise the many ways in which your customer information gets used or disclosed.

It will be important to identify carefully the purposes for which personal information is being used. Use is the key factor because your organization will only be allowed to collect information which is necessary for the purposes for which your organization uses it and your organization will have to specify the purposes for which it is going to be used when your organization is collecting it from the individual. If your organization subsequently changes the purpose or adds a new purpose you will likely have to go and get a new consent.

What Is Consent?

No personal information can be collected, used or disclosed without knowledge and consent except in those limited circumstances contemplated by C-6. Consent can be given orally or in writing. It would appear that negative options can be employed and there is probably room for an implied consent.

Consent must be informed and must be directed not only to the fact that the information is being collected but to the uses to which it is to be put.

An interesting question arises as to whether the degree of informed consent required will vary with the nature of the information being requested. Collecting an individual's name, address and telephone number for the purposes of a magazine subscription may not require any consent other than the fact that the individual sends in his or her request for the magazine. The very act of subscribing implies that the individual is consenting to the information being used for the purposes of mailing the magazine and probably would include purposes related to correspondence necessary for billing and renewal. On the other hand, with highly sensitive information such as medical information, credit card numbers and other financial information a more specific and detailed consent process will be required.

What Can We Collect?

C-6 makes it clear that the scope of the information collected is limited to that which will be necessary for the purposes identified. To use the magazine subscription example, while name and address are necessary for the purposes of the magazine subscription activities, is the telephone number necessary? Is the age of the subscriber or the gender of the subscriber necessary? These additional pieces of information are no doubt extremely important for the demographic profile that the publisher would like to build with respect to its subscribers, but the information is presumably not necessary for subscription purposes. In such circumstances, the publisher would be obliged to expand its identified purposes to include the establishment of a demographic profile of its subscribers for the purposes of selling advertising or soliciting reader-appropriate articles.

How Far Do Our Responsibilities Go?

If your organization collects personal information, your organization becomes responsible for it. If your organization outsources data processing or enters into contracts which require the handling of personal information collected by your organization, be sure that it is a term of any such outsourcing agreement or contract that the other party will abide by the requirements of C-6, including collection, use and handling of the personal information. Your organization will also want to obtain an indemnity with respect to any costs or damages award arising out of a breach by the other party.

Can I Throw It Out?

Another facet of C-6 pertains to the retention of personal information. Personal information is not to be retained after it is no longer required to fulfil the purpose for which it was collected. On the other hand, corporate policies with respect to the destruction of information will have to take into account that information cannot be destroyed during the course of an inquiry from an individual or during the course of an investigation by the Privacy Commissioner. Records management policies and procedures will have to be developed on the basis of a recognition of the principles regarding the limitations on use of personal information and the requirement not to retain the information after it has served its stated purpose.

What If It's Wrong?

The requirements of C-6 with respect to the accuracy of information may appear somewhat contradictory. There is an obligation on the part of an organization to ensure that personal information is as accurate, complete and as up to date as is necessary for the purposes for which it is being used. On

the other hand, an organization is not to update personal information routinely unless it is necessary for the purposes for which the information is to be used. The guideline is whether the information is accurate enough to minimize the possibility that a decision about the individual will be based on inaccurate information. The requirement that the information be as accurate as is reasonably necessary for the purposes for which it is to be used also requires the establishment of a mechanism whereby an individual can complain about the inaccuracy of information and request a correction. This is discussed below.

Where Should I Keep This Stuff?

The guiding principle enshrined in C-6 with respect to the security of personal information is that it "shall be protected by security safeguards appropriate to the sensitivity of the information". Again there is a recognition that there are varying degrees of privacy attached to personal information. Once again policies and procedures will have to be developed for staff in order to ensure that personal information is provided only to those who have a requirement to use it and that storage is appropriate. Physical storage of such information is probably fairly straightforward. Certainly most organizations will already have in place appropriate safeguards to deal with the personal information of their employees. On the other hand, other information regarding customers or subscribers may not be routinely protected unless it is considered proprietary or confidential by the organization.

Obviously, one of the most difficult areas to come to grips with is the area of computer generated and stored personal information. Again it is likely that most organizations will be required to conduct some sort of audit of their personal information handling practices in order to ascertain what security measures will be appropriate for their personal information holdings. Indeed, one of the obligations imposed by C-6 is to make readily available to individuals specific information about the policies and practices that your organization has adopted with respect to the management of its personal information holdings, including:

- The name or title and the address of the person who is accountable for your organization's policies and practices and to whom complaints or inquiries can be forwarded.
- The means of gaining access to personal information held by your organization.
- A description of the type of personal information held by your organization, including a general account of its use.
- A copy of any brochures or other information that explain your organization's policies, standards or codes and what personal information is made available to related organizations such as subsidiaries or sister corporations.

Can I Find Out What They Know About Me?

Part of your organization's personal information management practices will have to include the establishment of a mechanism whereby an individual can obtain access to his or her personal information held by the organization. As indicated earlier, if the individual is not satisfied with the accuracy of the information he or she will have to be given an opportunity to challenge it and have the information amended as appropriate. Your organization must provide a user friendly process and assist individuals who ask for help in accessing information and preparing the appropriately worded request. Once your organization has received a request it has 30 days to respond although it can extend that by a further 30 days. Your organization can charge "minimal" fees for processing a request if it informs the individual ahead of time what the fees will be and, if the information is going to be refused, it must refuse in writing and provide reasons for refusing access to the information.

The bases on which your organization may refuse to disclose personal information to an individual who makes a request would include the fact that the information is also information about a third person who has not consented; it is subject to solicitor-client privilege; the information could be considered proprietary and its release would reveal confidential commercial information; providing access to the personal information would threaten the life or security of another individual; the process of providing access to the information would be prohibitively expensive; the information was collected in a reasonable manner for purposes related to the investigation of a breach of an agreement or a contravention of the laws of Canada or a province; or the information was generated as the result of a formal dispute resolution process including a court case. The right to refuse to disclose information is severely limited and where it is possible to do so the information should be severed so that as much personal information as possible can be released without compromising the other information.

What If The Individual Is Not Happy?

The Code and C-6 combined provide for a fairly elaborate system of appeals for an individual who is not satisfied that an organization has complied with C-6 or the Code. The organization itself must put in place a procedure to receive and respond to complaints or inquiries. The organization is responsible for advising individuals about the external complaint process that may follow and must have a mechanism for legitimately dealing with and investigating complaints. If the individual is

not satisfied with the response of the organization he or she may complain to the Federal Privacy Commissioner that there has been a contravention of either C-6 or the Code. Any complaint has to be made within six months but there is a mechanism for extensions.

The Office of the Privacy Commissioner is the agency currently charged with the oversight of the application of the federal *Privacy Act* to the federal government and its agencies. The resources of the Privacy Commissioner are already strained by the number of complaints received and investigations required in that context. It appears that the government has dedicated additional resources to the Privacy Commissioner in response to the passage of the Act, but it remains to be seen whether they will be sufficient to allow him to undertake, in a meaningful way, the role that has been assigned to him by C-6. The Commissioner has wide-ranging investigative powers including the ability to enter premises at reasonable times without any prior judicial authorization and the power to issue subpoenas. The Commissioner has no formal powers to make orders but he is expected to engage in mediation and dispute resolution processes and, in most cases, issue a report setting out the findings of any investigation that he has undertaken.

The Commissioner also has the right to audit the personal information management practices of an organization even though he may not have received a formal complaint. The only requirement is that he have reasonable grounds to believe that the organization is contravening a provision of C-6 or not following a recommendation in the Code.

If a complainant is still not satisfied after a report is issued by the Privacy Commissioner he or she may apply to the Federal Court for a further hearing. The Commissioner also has the right to initiate a hearing before the Court. The Court can order an organization to correct any personal information handling practice that is not in compliance with C-6 or the Code and can award damages. It is interesting to note that the review jurisdiction of the Federal Court in respect of the personal information handling practices of the federal government does not include any similar power on the part of the Court to award such damages.

Can I Avoid This Legislation?

It is possible that in some circumstances organizations may be able to avoid the immediate application of C-6 by altering their personal information management practices. For example, your organization may be caught because the personal information which it uses is stored and processed at a data centre located in a province or country other than the jurisdiction in which it carries on its business. As previously noted, for the first three years of the life of C-6 it will not apply to organizations which collect, use or disclose personal information within individual provinces unless it pertains to the operation of a federal work, undertaking or business. Your organization might be able to buy some time by moving the location of its data processing facility from one province or country to another.

In our view, the passage of C-6 or similar legislation was inevitable. Unless Canada had put in place its own laws providing for comprehensive protection for personal information, Canadian businesses would have found themselves at a distinct disadvantage when dealing with EU states. Having said this, it is distinctly possible that the eventual application of C-6 to provincially regulated businesses will result in a constitutional challenge by a province or by an affected, provincially regulated business. It is our understanding that the federal government is relying, at present, upon the federal trade and commerce power contained in the *Constitution Act* (1867) to justify what would appear to be a complete incursion into matters which are otherwise under the constitutional control of the provinces. The legal soundness of this approach has yet to be tested.

For more information, contact the authors at McCarthy Tetrault's Ottawa office: 613-238-2000

UPCOMING SEMINAR

The Insurance Institute of Ontario and the Insurance Council of Canada presents:

New Federal Privacy Law C-6: Personal Information Protection and Electronic Documents Act

The new federal privacy law will impact how insurers conduct their business. Certain information practices will be affected in January 2001, while general compliance with the new law will be required by January 2004. This seminar will provide front-line insurance industry employees with practical information and advice to recognize and manage privacy issues that arise in their dealings with policyholders and claimants. Participants will receive a copy of C-6, a copy of the IBC privacy code, implementation checklist and copies of presentation data.

Date: Tuesday August 15, 2000
Time: 9.00 a.m. to 12.00 p.m.
Location: Canadian Bar Association, 20 Toronto Street, ON
Registration: Jennifer Marshman, 416-362-8586 ext. 244 or email jmarsh@iic-iac.org