Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act*

Case Examples

National Privacy and Access Law Section
Canadian Bar Association

December 2005

865 Carling Avenue, Suite 500, Ottawa, Ontario K1S 5S8
Tel/Tél: 613 237-2925 Toll free/Sans frais: 1 800 267-8860 Fax/Télécop: 613 237-0185
Home Page/Page d'accueil: http://cba.org/abc E-mail/Courriel: info@cba.org

TABLE OF CONTENTS

Preparing for the 2006 Review of the Personal Information *Protection and Electronic Documents Act*

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the National Privacy and Access Law Section of the Canadian Bar Association, with assistance from the Legislation and Law Reform Directorate at the National Office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the National Privacy and Access Law Section of the Canadian Bar Association.

Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act*

I. INTRODUCTION

In its recent meeting with Industry Canada officials, the National Privacy and Access Law Section (the CBA Section) was asked to provide case examples to support several of the specific recommendations in the Section's submission entitled "Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act*".[1]

The following case examples and accompanying analysis are keyed to the headings and enumerations in the Section's earlier submission.

II. DEFINITIONS

A. Commercial Activity

Issue

Need to clarify activities of non-commercial entities that are of a "commercial character".

Examples

The Assistant Federal Commissioner recently held that a non-profit daycare centre that is subsidized, but not operated, by a municipality is engaged in commercial activity when it charges its clients for the provision of daycare services.[2] On the other hand, a recent decision of Ontario's Superior Court of Justice held that a mere exchange of consideration is not enough to create "commercial activity" for the purposes of the Act.[3] The Court

1 (Ottawa: CBA, August 2005).

2 PIPEDA *Case Summary* #309: *Daycare denied parent access to his personal information*, April 18, 2005, online: http://www.pfrivcom.gc.ca/cf-dc/2005/309_20050418_e.asp.

3 *Rodgers v. Calvert* (2004), 2004 Carswell Ont. 3602 (S.C.J.).

concluded that such a non-profit association is not engaged in commercial activity when it provides services and other benefits of membership in exchange for a membership fee.

Analysis

It may be impossible to create a definition of "commercial activity" that will permit a straightforward and unerring characterization of a particular dealing with personal information as being either commercial or non-commercial for the purposes of the Act. However, it should be possible to list certain types of activity that are not commercial, and others that are in the definition of "commercial activity". A possible model is in the definition of "personal information" found in the federal *Privacy Act*.

III. APPLICATION

A. Clarifying the Scope of Employee Information Excluded from PIPEDA

Issue

Need to delineate the line between personal information that is not employee personal information of non-federal works, undertakings or businesses (non-FWUBs) and employees and their employee personal information.

Examples

Is a non-FWUBs employer that provides an employee list to an issuer of corporate credit cards for marketing purposes in return for a reduced rate on corporate card services subject to the Act with respect to that transaction? As another example, do non-FWUBs employers' disclosures of employee personal information to group benefit providers fall within the ambit of the Act?

Analysis

As is the case with the definition of commercial activity, it would be difficult to precisely define the distinction between the non-FWUBs employee data excluded from the scope of the Act and that included. Adding express language to the Act to clarify the points of demarcation between the two categories would facilitate compliance.

IV. SPECIFIC EXCEPTIONS TO THE REQUIREMENT FOR CONSENT

B. Reciprocal Collections and Disclosure Rules

Issue

The lack of parallelism and similar treatment for information that may be collected and disclosed pursuant to the specific rules contained in subsections 7(1) and (3) of PIPEDA.

Example

A property insurer is seeking to process a claim by its insured that involves potential settlement and payment to a third party (i.e. party who is not a customer of the insured). The insurer is concerned that the third party claim may be fraudulent and wishes to obtain information respecting prior claims made by this party. Such information is available in insurance industry databases and potentially from the third party's insurer directly. Under paragraph 7(1)(b), the first party insurer may collect such information. However, there is no commensurate permission for the third party's insurer, or the industry database organization, to disclose the information directly to the insurer. The only avenue open is to disclose the information to an investigative body that then is entitled to disclose it to the insurer.

Analysis

There is no direct "other side" to the insurer's right to collect the information without consent. Informally, staff at the Office of Privacy Commissioner have suggested that such a right should be implied. However, this interpretation is not clear from the legislation. A straightforward provision is found in the Alberta and B.C. PIPAs, where the exception for collection without consent is mirrored in the exception for disclosure without consent. Such a provision should be added to PIPEDA.

C. Required or Authorized by Law

Issue

The exception for disclosure without consent (paragraph 7(3)(i), PIPEDA) does not encompass disclosures that are authorized – but not required – by another statute. Further, it does not address the scope of the word "law".

Example

Collection and disclosure of credit information for the purposes of approval of a loan application is permitted by certain provincial consumer/credit reporting legislation without the consent of the applicant. Generally this information is collected and provided by consumer reporting agencies. However, PIPEDA would not permit such disclosure without the individual's consent.

Analysis

The general principle that should be followed is that if another statute (federal or provincial) permits the collection or disclosure without consent, that rule should be recognized by PIPEDA. PIPEDA should not attempt to (and arguably may be found not to) restrict or create different rules from those existing under separate statutory regimes.[4] A provision similar to the PIPAs would address this issue.

E. Litigation

Issue

Should the collection, use and disclosure of personal information in relation to the litigation process be governed by PIPEDA?

Example

A very recent example in PIPEDA Case Summary #311 illustrates the difficulty of applying PIPEDA to information collected, used and disclosed in the course of litigation. A number of court decisions have grappled with the same issue. In this case summary, the plaintiff complained that her personal information was collected by the defendant insurance company through surveillance. The information was used in court and determined by the court to be "relevant". In this finding, the Privacy Commissioner, using implied consent, held that the collection of the personal information was authorized, but only to the extent that it is "relevant" to the merits of the case.[5]

4 The analysis in the Ontario *Ferenczy* case is pertinent in this regard.

5 PIPEDA *Case Summary* #311at 2.

Analysis

Courts in litigation determine relevancy and are better placed to do so in light of their full knowledge of the action. If the Privacy Commissioner also makes such determinations, there is not only a risk of contradictory rulings, but also an erosion of the traditional jurisdiction of the courts to have carriage of an action. As in comparable legislation in BC (section 3(4)) and Alberta (section 4(5)), an exclusion should ensure that the legislation does not impact on the litigation process. The Alberta model is preferable in its breadth, but neither fully addresses the issues. Personal information collected, used or disclosed in relation to litigation should be excluded, or an exception in section 7, based on similar wording, could be added.

V. THIRD PARTY PROCESSORS, AGENTS AND INVESTIGATIVE BODIES

A. Third Party Processor

Issue

Is a third party processor considered to be part of the client organization for the purposes of PIPEDA, such that the processor can collect, use and disclose on behalf of the client (to the extent the client could itself do so under PIPEDA) without additional consent identifying the role of the processor (the broader interpretation)? Alternatively, is the role of the processor limited only to receiving personal information from its client, processing same, and returning it to the client (the restrictive interpretation)?

Example

If, using the restrictive interpretation, a third party processor can only literally "process", or use, personal information in the operation of a contest, but cannot collect or disclose such information without obtaining additional consent, then an organizer seeking to operate a contest would have two options if it wished not to specifically identify the third party processor on the contest form: (1) collect the information itself from contestants, provide it to a third party vendor to process the information to determine a winner, receive that information back, and itself disclose the identity of the winner to media outlets, etc. to publicize the contest; or (2) as is the more normal case, engage a contest fulfillment house

to perform all of these functions: i.e. collect the contestant applications, use the information to determine a winner, and disclose the winner's identity in connection with the publicizing of the contest.

Analysis

Identifying the processor would result in no additional protection for each individual contestant, and the third party processor concept does not require the organizer to identify the fulfillment house in the contest application form. Identifying the processor in the consent could become particularly problematic where a transaction may involve multiple processors (e.g., in connection with the approval of a mortgage).

D. Investigative Bodies

2. Disclosure Consent Exemption for Investigations (Disclosure to Investigative Body)

Issue

Should there be a reciprocal disclosure exemption in section 7(3) to parallel the collection exemption in section 7(1)(b) permitting collection without consent if reasonable for purposes relating to a breach of an agreement or contravention of laws?

Example

An insurance company investigating an insured's claim seeks to collect personal information from the insured's employer under section 7(1)(b). To obtain the personal information, the company has to provide some context as to why they are requesting such information, which involves disclosing some personal information to the employer. Two significant problems result:

(1) There is no disclosure consent exemption in section 7(3) that permits the insurance company to disclose this information to the employer. (the first disclosure)

(2) There is no disclosure exemption that allows the employer to disclose personal information to the insurance company, despite the existence of a collection exemption that permits the company to collect such information from the employer. (the second disclosure)

Analysis

The insurance company could only conduct the first disclosure by retaining an "investigative body", such as a private investigator, who could then disclose the personal information to the employer on behalf of the company under section 7(d). Similarly, if the insurance company retains a private investigator, the employer could disclose the personal information to that investigator under section 7(d) (subject to the awkward requirement that the disclosure be made "on the initiative" of the employer). As a result, the insurance company is forced to engage a private investigator to complete tasks that the company should be able to perform itself. This imposes unnecessary costs on the insurance company, and effectively provides no additional protection to the individuals in question.

VI. ACCESS REQUESTS

A. Applicable to all Exemptions

B. Investigations of Breaches of Law or Agreement

C. Formal Dispute Resolution

G. Settlement Privilege

Issues

Exemption for law enforcement investigations--are the provisions too complex to be workable and would the targets of the investigation be able to discern sensitive information simply by virtue of the limited responses available to organizations?

Formal dispute resolution-- what is this and would it include settlement privilege? Solicitors' liens--should access be provided even where under other legislation the file would not be accessible to the client (for non-payment, etc.)

Litigation process--where information is exchanged in discoveries subject to the implied undertaking of confidentiality, should it be accessible under this legislation?

Examples

A target of a CSIS investigation makes a request for his or her own records and is turned down, but the legislation allows for delays to get further direction / information from CSIS etc. Since no other exemption operates that way, the target knows he or she is the target, and acts accordingly.

In an action, counsel discusses possible settlement with the other side, and the discussions include sharing information about a named witness. The witness makes an access request and argues that such discussions are not "formal dispute resolutions" as in mediation or arbitration.

Legislation prohibits a client from getting access to his or her file because the legal account has not been paid. The client circumvents that legislation by making an access request for the personal information contained in the file.

In discoveries, information is exchanged under the implied undertaking rule. A witness named in the documents makes an access request for his or her own personal information. Such information is not solicitor client privileged, and unless subject to some other exemption, would be disclosed.

Analysis

The difficulty is the complexity of the provisions and the failure to include a "refuse to confirm or deny the existence of the record" provision--such as are common in public sector legislation like Ontario's FIPPA (sections 14(3) and 21(5)) for law enforcement and personal information exemptions. However, it cannot only be available for this exemption, since that would disclose what the issue is for such requesters. To address the complexity and the problem of unintended disclosure or confirmation of information about investigations, an exemption that would apply where another statute or government agency prohibits disclosure may address the issue and would greatly simplify the process.

Formal dispute resolution--the exclusion for litigation, as noted above, would address this issue. However, if that is not done, then all records in relation to settlement discussions or

dispute resolution ought to be exempt to encourage settlements and to conform with the common law.

Where no access would be available by virtue of the operation of another statute, there ought either to be an exemption, or as in BC, an exclusion if it is expressly noted to prevail (section 3(5)).

As above, records collected, used or disclosed in relation to the litigation process may simply be excluded. Alternatively, an exemption to that effect that expressly addresses the implied undertaking process in language similar to Alberta's section 4(5) is recommended.

F. Substitute Decision-Makers

Issue

There is no provision that enables a person acting for a minor, a deceased person or other person who has legally given an authorization, e.g. power of attorney, to request access to that second person's information.

Example

An insurance company receives a request from the executor (or spouse who is not an executor) of a deceased policyholder for information respecting the policy.

Analysis

PIPEDA contains no clear provision that directs the company to the proof of authority required. Currently, the company must extrapolate from provincial legislation respecting the authority of personal representatives, which does not directly address the issue. A provision should be added to PIPEDA to clarify this authority.

VIII. CONSENT ISSUES

B. Third Party Consent

Issue

Should PIPEDA explicitly address the issue of consent obtained indirectly from an individual through another organization or individual?

Examples

There are many circumstances where consent is not obtained directly from the individual whose personal information is being collected, used or disclosed:

- an individual may be asked to provide personal information about a family member, guarantor or other person close to them (e.g. an applicant for a loan may be asked to provide certain personal information about their spouse and to indicate that the spouse's consent has been obtained; a student may be asked to provide personal information about their parent or guardian)

- organization A may disclose personal information about an individual to organization B based on a consent to such disclosure given to organization B as part of an application process (e.g. a credit bureau discloses personal information about an insurance applicant to an insurance company based on the insurance company's representation that it has received consent from the applicant for the provision of the information; a former employer of an individual discloses personal information to a prospective employer based on the prospective employer's representation that the former employee has consented to the disclosure as part of the job application process)

- organization A may collect personal information about an individual from organization B based on a consent to such collection given to organization B as part of an ongoing business relationship (e.g. a credit bureau collects information about an individual from a bank or credit card issuer as a result of a consent to such collection given by the individual in a loan or credit card agreement; a company collects personal information of an individual in order to send marketing material that the individual has consented to receiving during the course of entering a contest run by an affiliate of the company)

Analysis

In all of the examples above, consent to the collection, use or disclosure of the individual's personal information is not given directly to the organization that actually performs the collection, use or disclosure. That organization must rely on a representation (explicit or implied) made by the organization or individual that has a direct relationship with the individual whose information is being collected, used or disclosed that appropriate consent has been obtained. While in some circumstances, the person communicating the consent to the entity could be considered the other individual's agent, this would not always be the case.

At present, PIPEDA does not address such indirect consent situations. The Privacy Commissioner of Canada has recognized that consent can be obtained in this way. For example, in Decision #188, the Commissioner stated that "it was reasonable for the credit agency to obtain the consumer's consent through its client businesses and not directly, given the large number of information requests it receives daily and the considerable amount of work this type of procedure could involve". However, in Decisions #266 and #246, the Commissioner stated that a bank could not rely on a consent to a credit check given to another bank which was subsequently merged with her current bank. Little guidance has been given by the Commissioner to allow companies to determine when they can rely upon third party consent representations.

An organization should be explicitly permitted to rely, acting reasonably, on an assurance or on surrounding circumstances that a person providing personal information of another individual has consent of the other individual for the specific purposes involved, or that the other individual would consent if aware of the circumstances (a donation or gift). Factors in assessing the reasonableness of this reliance include the nature of the transaction, the sensitivity of the personal information, whether the collection, use or disclosure benefits the individual, the nature of the relationship between the individual and the person confirming the individual's consent, and apparent authority given by one individual to deal with another individual. They should be explicitly listed, although the list need not be exhaustive.

C. Consent by Minors

Issue

Should PIPEDA address in more detail the issue of consent obtained from minors?

Examples

There are many instances where consent is required for the collection, use and disclosure of personal information of minors. The nature of the specific situation in which such consent is required may call for differing responses:

- A minor's consent may be required for the collection, use and disclosure of sensitive personal information about the minor, such as health information. In most cases, it would likely be reasonable to require that the parent or guardian of the minor be required to consent to such collection, use and disclosure.

- A minor's consent may be required for the collection, use and disclosure of personal information in the course of commercial dealings undertaken by a minor, such as opening a bank account or obtaining a credit card. While older minors in their teen years should likely be able to provide the appropriate consent, it is arguable that the consent of a parent or guardian should be required for children below a certain age.

- A minor's consent may be required for the collection, use and disclosure of personal information in the course of non-commercial transactions such as contests and other promotions. Many of these transactions are carried out online, where it is difficult to efficiently confirm the age of a participant. Again, while older minors in their teen years should likely be able to provide the appropriate consent, it is arguable that the consent of a parent or guardian should be required for children below a certain age.

- It is also important to note that any age restrictions that are built in to the consent requirement should be based on a reasonable good faith belief of the organization seeking the consent about the age of the individual providing the consent.

Analysis

PIPEDA gives little guidance about how the consent of minors can or should be obtained. The only possible reference to minors in PIPEDA is in Principle 4.3.6, which states that an authorized representative, such as a legal guardian or a person having power of attorney, can provide consent on behalf of an individual. Presumably this would apply to consent by a minor. It is unclear, however, whether a minor (as defined by provincial statute) can ever give consent personally. If they cannot, then organizations will be required to impose cumbersome and impractical consent mechanisms for obtaining routine consents from teenagers for the use of their non-sensitive information. On the other hand, if minors can, in fact, provide valid consent in some circumstances, those circumstances should be explicitly stated.

PIPEDA should be clarified to confirm that some minors can in fact consent to some collection, use and disclosure of their personal information if:

- they understand the nature of their action and the consequences of giving consent

- they are above a minimum age below which consent may not be given (such a restriction is contained in the Canadian Marketing

Association guidelines regarding marketing to children and teenagers and the U.S. *Children's Online Privacy Protection Act*, both of which state a minimum age (13) below which valid consent must be given by a parent), and

- the information is not of such a sensitivity that consent of a parent or guardian (if one exists) should be required or sought.

IX. DISCLOSURES OUTSIDE OF CANADA (OUTSOURCING)

Background

Since the CBA Section's earlier submission, the Office of the Privacy Commissioner has released Finding #313, in which the Assistant Commissioner acknowledged that, notwithstanding significant concerns regarding the U.S. *Patriot Act*, personal information held by an organization that could be obtained by government authorities was at comparable risk in either the US and Canada. However, the Assistant Commissioner reaffirmed the Office's position that "a company that outsources information processing to the United States should notify its customers that the information may be available to the U.S. government or its agencies under an order made in that country". We understand that the position of the Office is that a company that outsources information processing outside of Canada should generally notify its customers.

Issue

Should organizations be required to notify individuals if their information may be used or held outside of Canada?

Example

A Canadian company with customer offices in Canada hosts its data management centre in Germany, which in turn keeps its back-up "hotsite" in neighboring France, and outsources its customer call centre to India. As a result, customer information either is or has the potential to be used, held or disclosed in multiple jurisdictions outside Canada.

Analysis

Should all three jurisdictions be highlighted in the notice? Can the company draw a distinction between those European countries which have implemented the Data Protection Directive through the enactment of national privacy legislation, and India which has little to no data protection legislation? If the company is required to also identify Germany and France in its notice, what does that mean for the adequacy principle? More specifically, does it suggest that while the EU has deemed Canada "adequate" for the purposes of the Directive, Canada has effectively not deemed the EU to be adequate for the purposes of PIPEDA?

We note that the notification requirement reaffirmed in Finding #313 in regard to information going to the US for processing seems potentially at odds with the Assistant Commissioner's acknowledgment of a comparable legal risk of either the Canadian or the US government obtaining personal information.

We suggest that this concern might be alleviated by ensuring that:

(a) if the extra- jurisdiction processor is a third party, each organization imposes the appropriate contractual obligations on the vendor, or
(b) if the extra-jurisdictional processor is a related party, it implements appropriate safeguards and/or is bound by appropriate contractual obligations.

X. CONCLUSION

We trust that these specific examples will help to illustrate issues raised in this and the CBA Section's earlier submission. We look forward to continuing to be involved in the 2006 PIPEDA Review.