Corporate/Commercial Law Reform in Ontario:
Tomorrow's Business Law

PRIVACY LEGISLATION: IMPACT ON BUSINESS TRANSACTIONS AND THE NEED FOR REFORM

Bruce McWilliam
McMillan Binch Mendelsohn LLP

Monday, May 16, 2005

Ontario Bar Association

PRIVACY LEGISLATION: IMPACT ON BUSINESS TRANSACTIONS AND THE NEED FOR REFORM

1. Introduction

Although privacy issues have arisen from time to time in the past, recently privacy has emerged to become an important issue in many aspects of life, impacting us in a number of ways, including as consumers and in how we conduct business. More and more, headlines seem to deal with things like stolen hard drives, misdirected faxes, identity theft, post 9/11 national security issues, and so on.

At the same time, business transactions continue to take place. Crosbie & Company Inc. has reported that 859 announced merger and acquisition transactions valued at a total of $115 billion took place in Canada in 2004[1].

A large number of these, and many other types of transactions, involve the transfer[2] of personal information. Many of these transactions currently take place in a context of uncertainty regarding how they are to be negotiated and completed while complying with applicable privacy laws.

This paper will discuss current Canadian privacy laws, how they impact business transactions, the ways businesses now try to comply with them, and how we might implement reforms while ensuring proper protection of personal information. Although there are numerous areas where privacy law reform may be advisable, this paper will concentrate on the transfer of personal information in business transactions.[3] In addition, the focus of this paper will be privacy legislation as it applies in Ontario. Certain references to other provincial laws will be made for comparison purposes.

2. Background

Canada's current privacy legislation derives largely from the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organization for Economic Cooperation and Development in 1980[4]. Canada formally accepted the guidelines in 1984, but in fact had implemented privacy legislation governing the public sector (the *Privacy Act*) several

---

[1] Crosbie & Company Inc., Press Release, *Canadian M&A Activity - Fourth Quarter 2004 Report, Market Firing on All Cylinders*, February 23, 2005, http://www.crosbieco.com/M&A_Press_Release_Q404_23Feb05.pdf

[2] In this paper, the term "transfer" is used as a neutral term, which will in some cases not be the same as "disclosure".

[3] Also, the issue of transfer of information out of Canada, most notably to the United States, and possible application of the *USA Patriot Act* to Canadian information, is outside the scope of this paper. For further discussion of this, see, for example, Office of the Privacy Commissioner of Canada, *Transferring Personal Information about Canadians Across Borders – Implications of the USA PATRIOT Act - Submission of the Office of the Privacy Commissioner of Canada to the Office of the Information and Privacy Commissioner for British Columbia*, August 18, 2004, http://www.privcom.gc.ca/media/nr-c/2004/sub_usapa_040818_e.pdf

[4] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

years before. Similar provincial legislation governing public sector agencies was put in place in subsequent years.

Adoption of rules governing the private sector followed. In 1994, Quebec implemented *An Act Respecting the Protection of Personal Information in the Private Sector*, which (with Civil Code articles 35 to 41) reflects many of the principles from the OECD Guidelines. In 1996, the Canadian Standards Association adopted its voluntary *Model Code for the Protection of Personal Information* modeled on the OECD Guidelines.

A major impetus for moving forward with privacy legislation in Canada was the European Union's Data Protection Directive[5] released in 1995, becoming effective in 1998. Among other things, this prohibits EU member countries from transferring personal information to non-member countries whose laws or other security measures do not ensure a level of protection comparable to that in the Directive.

Canada's response was the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). PIPEDA became effective for federally-regulated organizations engaging in commercial activities, and for all interprovincial and international transfers of personal information for consideration, on January 1, 2001. It essentially adopted the Canadian Standards Association Model Code, and in fact made the substance of that Code a schedule to the statute, with modifications of certain Code provisions implemented by specific sections in the body of the statute.

Effective January 1, 2004[6], PIPEDA applies to all organizations[7], including provincially-regulated ones, that collect, use or disclose personal information in the course of commercial activities, unless the province has passed a law substantially similar to PIPEDA. (With respect to employees, however, PIPEDA continues to apply to employees of only federally-regulated organizations[8].) Where a province has passed a substantially similar law, the Governor in Council may grant an exemption from PIPEDA for information dealt with exclusively within the province. To date, Quebec's statute, as well as the *Personal Information Protection Act* of each of British Columbia and Alberta, have been declared substantially similar[9], and so operate in place of PIPEDA within those provinces.

---

[5] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

[6] See PIPEDA, section 30.

[7] Subsection 2(1) of PIPEDA states that "organization" includes an association, a partnership, a person and a trade union.

[8] However, PIPEDA would probably apply, for example, to prospective employees and former employees of provincially-regulated organizations.

[9] Quebec - Canada Gazette, Part II, Vol. 137, No. 25 — December 3, 2003, SOR/2003-374, 19 November, 2003, *Personal Information Protection and Electronic Documents Act*, Organizations in the Province of Quebec Exemption Order, P.C. 2003-1842, 19 November, 2003 (see http://canadagazette.gc.ca/partII/2003/20031203/html/sor374-e.html)

Alberta - Canada Gazette, Part II, Vol. 138, No. 22 — November 3, 2004, SOR/2004-219, 12 October, 2004, *Personal Information Protection and Electronic Documents Act*, Organizations in the Province of Alberta Exemption Order, P.C. 2004-1163, 12 October, 2004 (see http://gazetteducanada.gc.ca/partII/2004/20041103/html/sor219-e.html)

PIPEDA and the substantially similar provincial statutes impose a number of obligations concerning personal information. For the purposes of this paper, the essential requirement is that personal information (i.e. information about identifiable individuals, other than the name, title or business address or telephone number of an employee of an organization[10]) cannot be collected, used or disclosed by an organization without the informed consent of the individual, subject to certain statutory exceptions. This applies equally to the use and disclosure of information collected by an organization before it became subject to PIPEDA.[11]

In early 2002, Ontario proposed draft privacy legislation which would be similar to PIPEDA - the *Privacy of Personal Information Act, 2002*[12]. This legislation was not implemented, although the *Personal Health Information Protection Act, 2004* (Ontario) was subsequently enacted to regulate how health information custodians, their agents and recipients may collect, use and disclose personal health information within the Ontario health care system.[13]

In contrast, the United States has taken an approach that does not involve comprehensive legislation, but instead uses a "safe harbor" framework approved by the EU. Organizations that wish to obtain safe harbor benefits must self certify annually that they comply with seven principles relating to: notice to individuals; opt-in choice for sensitive information, and opt-out choice for other information, for disclosure or new uses; restrictions on transfers to third parties; provision of access by individuals to their personal information; security; data integrity; and enforcement.[14]

3. The Current Situation

a) The Impact of Privacy Legislation on Business Transactions

As mentioned, PIPEDA requires knowledge and consent of the individual for any disclosure of personal information[15], subject to specified exceptions[16]. Organizations must make a reasonable

---

British Columbia - Canada Gazette, Part II, Vol. 138, No. 22 — November 3, 2004, SOR/2004-220, 12 October, 2004, *Personal Information Protection and Electronic Documents Act*, Organizations in the Province of British Columbia Exemption Order, P.C. 2004-1164, 12 October, 2004 (see http://gazetteducanada.gc.ca/partII/2004/20041103/html/sor220-e.html)

[10] PIPEDA, subsection 2(1).

[11] PIPEDA contains no special rules regarding such "grandfathered" information. In contrast, see *Personal Information Protection Act* (Alberta), subsection 4(4) and *Personal Information Protection Act* (British Columbia), subsections 3(2)(i), 14(b) and 17(b).

[12] See http://www.cbs.gov.on.ca/mcbs/english/56Y2UJ.htm

[13] The Governor in Council proposed on February 5, 2005 to exempt health information custodians to which this statute applies from the application of PIPEDA in respect of the collection, use and disclosure of personal information that occurs within Ontario. See http://canadagazette.gc.ca/partI/2005/20050205/html/regle4-e.html

[14] See http://www.export.gov/safeharbor/

[15] PIPEDA, Schedule 1, clause 4.3.

[16] PIPEDA, subsection 7(3).

effort to ensure that the individual is advised of the purposes for which the information will be used, and the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.[17]

PIPEDA does not have exceptions for business transactions such as asset sales, secured financings, securitizations and outsourcings. The question then arises whether it is necessary to notify individual customers and other individuals whose personal information would be transferred prior to or on completion of such a transaction, and obtain their consent to the transfer of their personal information.[18]

The privacy concern arises both at the due diligence and closing stages of the transaction. At the due diligence stage, a prospective purchaser of assets, for example, will want to examine customer and employee information in order to perform a proper examination of the target business, and to establish a value for it. Then, on closing, this personal information will have to be transferred to the purchaser as part of the implementation of the transaction.

There does not appear to be a clear answer to the question of notification and consent at the present time, and therefore businesses and their advisors must proceed in an atmosphere of some uncertainty and risk. As a practical matter, some or all of the following approaches may be taken to try to address this issue:

(i) Limit personal information transfers - The extent of personal information provided should be limited to that which is actually necessary. Some types of information are not considered personal information[19], and can be transferred without consent. However, in virtually all cases, significant personal information must be transferred. In some cases, de-identified or aggregated information can be provided at the due diligence stage, with little adverse effect on the effectiveness of the process. Of course, it would still be necessary to transfer the full information on closing.

(ii) Restructure the transaction - In some cases, privacy considerations may be one of a number of factors which, for example, favour a share sale rather than an asset sale.[20] However, in some cases (e.g. those involving entities other than corporations, or where less than all of the corporation's business is to be

---

[17] PIPEDA, Schedule 1, clause 4.3.2.

[18] This assumes that the transaction is more than the mere sale of the personal information itself; express consent would be required in the latter type of transaction in virtually all cases.

[19] PIPEDA, subsection 2(1) states that "personal information" means "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization". This definition has been interpreted quite narrowly. For example, in a finding dated December 1, 2004, the Assistant Privacy Commissioner of Canada stated that "As a business e-mail address is not specified in subsection 2(1), we must conclude that it is an individual's personal information for the purposes of [PIPEDA]". See http://www.mgblog.com/resc/GeistPCCSpamdecision.pdf

[20] While this may avoid a problem on closing, there is still a potential problem with providing personal information for due diligence purposes, which may constitute a use or disclosure.

transferred, or constraints on transfers of shares exist) this is not a possible approach. In addition, in some cases a transaction might be restructured to take place in a jurisdiction where the laws provide more certainty for transfer of personal information in business transactions.

(iii) Rely on prior consent - In some cases, express personal information consents (as may be contained in customer and employment agreements) and privacy policies[21] will have been prepared in contemplation of such business transactions, and express consent (or a reasonable basis for implied consent) will have been obtained for transfers in business transactions. However, even though this will become more prevalent in the future, as documents are drafted with this in mind, there will inevitably be some personal information not covered by such provisions.[22]

(iv) Obtain opt-in consent - This approach could be used, especially if the number of individuals concerned is relatively small, such as in the case of a few key employees, or a business having a relatively small number of customers.[23] In the case of employees this can sometimes be done at the time that offers of employment with the acquirer are made. In many cases, however, seeking consent will raise timing, due diligence and non-responsiveness problems, discussed below.

(v) Provide for opt-out consent - This avoids the problem of non-responsive recipients, but the other problems associated with opt-in consent remain.[24]

(vi) Rely on the "transfer for processing" provision[25] - This would generally apply in an outsourcing context, rather than an asset sale. It might also apply in some

---

[21] In contrast, some privacy policies may have made the claim that personal information will "never" be disclosed to third parties, potentially restricting the range of options available in a subsequent business transaction. See, for example, *FTC* v. *Toysmart.com*, Nos. 00-11341-RGS, 00-13995-CJK (D. Mass.), discussed at http://www.fenwick.com/about_fenwick/Privacy_Law_Resources.htm

[22] As well, some commentators have questioned whether such a consent may be too vague and therefore ineffective, since the identity of the purchaser and date of the transaction would be unknown at the time of consent. See, for example, Jenifer E. Aitken, *Avoiding Privacy Pitfalls in Business Transactions No Easy Task*, The Lawyers Weekly, Vol. 23, No. 31, December 12, 2003.

[23] This approach has apparently been required in certain U.S. bankruptcy cases; see, for example, *Attorney General Cornyn Gets Privacy Guarantees in Dr.Koop.Com Bankruptcy*, News Release of the Texas Attorney General, March 19, 2002, where op-in consent was required for the transfer of personal health information. See http://www.oag.state.tx.us/newspubs/newsarchive/2002/20020319drkoop.htm

[24] This approach is apparently used in U.S. bankruptcy cases involving less sensitive personal information; see, for example, Living.com, Inc. Bankruptcy Proceeding (AG v. Poulin), No. 00-12522-FM (Bankr. D. Tx) and Egghead.com, Inc. Bankruptcy Proceeding, No. 01-32125-SFC-11 (N.D. Cal. Bankr.), discussed at http://www.fenwick.com/about_fenwick/Privacy_Law_Resources.htm

[25] The sole reference to this in PIPEDA is in clause 4.1.3 of Schedule 1, which reads in its entirety: "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."

aspects of securitizations, e.g. servicing of transferred accounts receivable. In these cases appropriate contractual provisions must be agreed upon by the parties, including those requiring: personal information to remain the property of, and be processed for the benefit of, the transferor; the information to be used only for the purposes for which it was transferred; appropriate security, backup and business recovery arrangements to be in place, including restrictions on access and further transfers; access and audit rights in favour of the transferor; rectification, deletion or updating of information upon instructions from the transferor; and liability, indemnification and termination provisions[26].

(vii) Rely on the debt collection exception - Paragraph 7(3)(b) of PIPEDA allows disclosure without knowledge or consent for the purpose of collecting a debt owed by the individual to the organization. In a limited number of cases, such as the transfer of accounts receivable in asset sales and securitizations, it may be possible to argue that this would allow the transfer of personal information of the debtor to an acquirer.

(viii) Adopt an approach similar to the British Columbia and Alberta "business transaction" exceptions[27] - Such an approach would typically involve the following:

(1) for the purposes of due diligence, the parties would enter into an agreement under which the collection, use and disclosure of the personal information is restricted to those purposes that relate to the business transaction, and the information is restricted to that necessary for the parties to determine whether to proceed with the business transaction, and if the transaction proceeds, for the parties to complete the transaction;

(2) for the purposes of closing, there would be an agreement under which the use and disclosure of the information would only be for those purposes for which the information was initially collected, and the information would be restricted to that related solely to the carrying on of the business; and

(3) in either case, if the transaction is not completed, the transferee must either destroy the information or return it to the transferor.

This approach allows information to be disclosed at both the due diligence and closing stages. This has the advantage of providing appropriate protection for personal information before and after transfer, while allowing the transaction to

---

[26] See, for example, the CSA Workbook, *Making the CSA Privacy Code Work for You*, http://www.csa.ca/standards/privacy/default.asp?load=code&language=English - model%20code; and the Canadian Chamber of Commerce *Model Contractual Clauses for Transfer of Personal Information to a Data Processor*, http://www.chamber.ca/cmslib/general/modelclauses.pdf

[27] See *Personal Information Protection Act* (Alberta), section 22 and *Personal Information Protection Act* (British Columbia), section 20.

proceed without third party involvement, thus resulting in little if any interference with timing or with the business aspects of the transaction.

b) Problems with the Current Situation

(i) Implied Consent

In many cases the approach in section 3.a)(viii) above is taken, often in conjunction with one or more of the other approaches. This appears to be consistent with informal views expressed by various privacy commissioners' offices. However, except when transactions occur in British Columbia or Alberta, uncertainty will remain over whether this approach in fact satisfies the applicable legislation. In jurisdictions other than British Columbia and Alberta, since there is no express statutory authority for it, this approach would presumably have to be justified on the basis that there is implied consent for the transfer.[28]

The only reference to implied consent in PIPEDA is in clause 4.3.6 of Schedule 1, which states, in part: " …. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive …. ".

The Office of the Privacy Commissioner of Canada in a Fact Sheet[29] has stated:

> *The CSA Model Code says "Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual". This covers situations where the intended use or disclosure is obvious from the context and the organization can assume with little or no risk that the individual, by providing the personal information, is aware of and consents to the intended use or disclosure. Thus, where circumstances indicate that an individual has a certain understanding, knowledge, or acceptance, or certain information has been brought to the attention of an individual, consent might be implied. …. This will require a consideration of many factors, such as what information was provided to the individual, whether the purpose was identified, and whether the practices are common and widely known.*[30]

In the context of sensitive information, such as medical records and income records, the Fact Sheet states:

---

[28] In support of this, it could be argued that, since the British Columbia and Alberta statutes allow transfers of personal information without consent in the context of business transactions, so long as certain rules are followed, then since those statutes have been declared to be substantially similar to PIPEDA, it is reasonable to say that such transfers should be permissible under PIPEDA so long as similar rules are followed.

[29] Office of the Privacy Commissioner of Canada, *Fact Sheet - Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act*, http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp. While not legally determinative, such Fact Sheets provide valuable insight into the approach of the Privacy Commissioner on such issues.

[30] The quotation from the CSA model code is contained in the definitions section of the original code, which was unfortunately not included in PIPEDA.

> *In some cases involving sensitive information, the individual could reasonably expect the information to be used or disclosed for certain purposes. For example, the OPC supports the current practice of implied consent for uses and disclosures that are directly related to the medical care and treatment of an individual patient (the circle of care).*

Whether this would extend to the transfer of personal information or personal health information on the sale of a business such as a medical or dental practice, for example, could be debated.[31] Certainly the use of the information by the transferee would continue to be for the medical care and treatment of the individual, but would the purpose of the transfer itself be for medical care and treatment? Arguably disclosure would allow the continuation of care and treatment, and without disclosure, access to care and treatment might be reduced, which would be contrary to the interests of the individual.[32]

A recent case has provided some support for the concept of implied consent under PIPEDA. In *Ferenczy* v. *MCI Medical Clinics*[33], a case involving video surveillance in a public place for the purpose of defending a medical malpractice lawsuit, the court stated:

> *… in the circumstances here, (where the recording was in a public place), the plaintiff has given implied consent to the defendant to collect, record and use her personal information insofar as it is related to defending himself against her lawsuit. …. Consent is not a defined term under [PIPEDA], and there is no indication in the Act that consent cannot be implied.*[34]

This indicates that implied consent should be possible under PIPEDA. Whether as a factual matter, transfer of personal information in a business transaction context is sufficiently obvious to result in implied consent remains to be tested in court.

In contrast, the British Columbia and Alberta statutes, as well as the *Personal Health Information Protection Act, 2004* (Ontario) and the Ontario consultation draft of the *Privacy of Personal Information Act, 2002* all contain provisions providing for some form of implied consent, whether or not referring to it by that term.[35] The general approach is that the purpose

---

[31] See *Personal Health Information Protection Act, 2004* (Ontario), section 42 for rules regarding successors. See also G.W.S. Scott, Q.C., L. Wakulowsky, G.M. Saylor & S. Diamond, *The Personal Health Information Protection Act: Implementing Best Privacy Practices*, (Markham: LexisNexis Canada Inc., 2005).

[32] In contrast, see the Dr.Koop.Com Bankruptcy matter, referred to above at footnote 23, where (in a U.S. bankruptcy context involving a privacy policy that expressly prohibited any disclosures or sharing without consent) opt-in consent was required for sensitive information such as medical information.

[33] (2004), 70 O.R. (3d) 277 (Ont. S.C.J.).

[34] *Ibid*, at paragraph 31.

[35] See *Personal Information Protection Act* (Alberta), subsection 8(2) and *Personal Information Protection Act* (British Columbia), subsection 8(1), to be distinguished from opt-out consent, provided for subsection 8(3) of each of the Alberta and British Columbia statutes; *Personal Health Information Protection Act, 2004* (Ontario), subsections 18(2), 20(2) and 32(1)(b), to be distinguished from opt-out consent such as that in subsection 20(4); and the draft *Privacy of Personal Information Act, 2002*, subsection 8(5).

must be obvious to a reasonable person, or that it is reasonable that a person would voluntarily provide the information.

The basis for implied consent and the applicability of that concept to business transactions is not well-supported by PIPEDA in its current form. Possible amendments are discussed below.

(ii) Other Issues

To the extent other approaches are used, other problems arise. For example, transforming an asset purchase into a share purchase, or changing the jurisdiction of the transaction, have massive implications for the deal, and it would seem unfortunate if privacy considerations dictated the form of the transaction in this way.

Other approaches will affect timing. For example, de-identifying information or using opt-in or opt-out consents will delay full investigation of the target business from the due diligence stage to near or after closing. Seeking consent will affect the timing of disclosure of the transaction, and may come into conflict with business considerations or securities legislation. Finally, requiring opt-in consent, or providing the opportunity for opt-out consent, may delay closing.

As well, if opt-in consent is required from a large group (e.g. customers), there will be the problem of recipients who have no objection to the transfer, but for various reasons fail to respond.

Consent-based approaches will often require alternative purchase pricing mechanisms, i.e. earn-out mechanisms for customers (and potentially employees) who agree to the transfer between agreement signing and closing, or after closing.

Certain approaches, such as reliance on the "transfer for processing" or debt collection provisions, will be available only in a limited range of situations. (The "transfer for processing" provision is discussed further below under the heading "Outsourcing".) As well, use of the debt collection exception could be met with the argument that the disclosure is not for the purpose of collecting the debt, but rather to accomplish some other business purpose, and thus does not come squarely within the exception.

In addition to the foregoing issues, jurisdictional issues will arise, resulting in uncertainty as to which statute or statutes will apply to a transaction. This will arise most often when transactions cross provincial or national borders. For example, in a transfer of personal health information from Ontario to a private sector organization in British Columbia, will the *Personal Health Information Protection Act, 2004* (Ontario), the *Personal Information Protection Act* (British Columbia) and PIPEDA all apply? To the extent that statutes impose different rules, increased complexity, uncertainty and compliance costs will result.[36]

---

[36] See, for example, the discussion in Office of the Privacy Commissioner of Canada, *Fact Sheet - Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts* (*PIPA*s), http://www.privcom.gc.ca/fs-fi/02_05_d_26_e.asp; Christopher S. Wilson and Jeffrey F. Vicq, *Exempting B.C. and Alberta: Stitching the Seamless Continuum*, Canadian Privacy Law Review, Vol. 1, No. 9, June 2004, at pages 101-105; and Brian C. Keith, *Cross-Canada Privacy Check-up: Recent Critical Developments Under PIPEDA*, Ontario Bar

(iii) Outsourcing

One particular type of transaction that raises special issues is outsourcing. Outsourcing can take different forms and can involve different aspects of a business's operations. However, in most cases personal information, whether that of customers, employees or others, is transferred from the outsourcing customer to the outsourcing services provider.

Outsourcing does not seem to be included in the various "business transaction" statutory exceptions. For example, in the British Columbia statute, "business transaction" is defined as "the purchase, sale, lease, merger or amalgamation or any other type of acquisition, disposal or financing of an organization or a portion of an organization or of any of the business or assets of an organization"[37]; in the Alberta statute, it is defined as "a transaction consisting of the purchase, sale, lease, merger or amalgamation or any other type of acquisition or disposal of, or the taking of a security interest in respect of, an organization or a portion of an organization or any business or activity or business asset of an organization and includes a prospective transaction of such a nature"[38]. The *Personal Health Information Protection Act, 2004* (Ontario) talks only of transfers to "successors" of a health information custodian[39]. The Ontario consultation draft of the *Privacy of Personal Information Act, 2002* made reference to business transactions, but contained no definition.

While some types of outsourcing transactions may have components that fall within such definitions, given the ongoing service provision aspect of most outsourcing arrangements, they will not fall squarely within these provisions.

As discussed above, the "transfer for processing" provision in PIPEDA seems to apply to outsourcing.[40] However, this arguably is intended to impose responsibility on the transferor for information transferred to a services provider, rather than providing any authority to actually perform the transfer.

Also of interest is whether such a "transfer for processing" is a "disclosure" for the purposes of PIPEDA. Tied into this issue is whether the use of personal information by the services provider should be considered as use by the transferor, either as "agent" or otherwise.

PIPEDA itself offers little if any guidance on these points. However, in a speech to the General Meeting of the Private Investigators Association of British Columbia on March 20, 2003, former federal Privacy Commissioner George Radwanski interpreted PIPEDA as allowing transfers

---

Association 2005 Institute of Continuing Legal Education, *Privacy - Hot Issues for Business Lawyers and Litigators*, February 3, 2005, at pages 33-35.

[37] *Personal Information Protection Act* (British Columbia), subsection 20(1).

[38] *Personal Information Protection Act* (Alberta), paragraph 22(1)(a).

[39] Section 42.

[40] PIPEDA, clause 4.1.3 of Schedule 1.

without express consent, as distinguished from disclosures, for standard business practices, and subject to conditions, with the transferee acting as agent for the transferor. He stated:

> *The Act allows an organization to transfer personal information to a third party, without consent, for processing purposes. Take, for example, a bank that wants to have cheques printed for its customers. The Act allows it to transfer personal information of its customers to a cheque printing company for this purpose.*
>
> *Notice that I didn't say that the bank is "disclosing" the information. That's because the Act distinguishes this kind of transfer for processing purposes from disclosures.*
>
> *Transfers are only allowed for limited purposes, and they're subject to stringent conditions. For instance, the processor can use the information only for the specified purposes, and has to protect the information as required by the Act.*
>
> *But the point I want to stress is that this recognition of transfers for processing, as distinct from disclosures, is necessary to the reasonable functioning of standard business practice. Considering this transfer as a "disclosure," and requiring banks to get the consent of their customers to it, wouldn't serve any useful purpose.*
>
> *In my view, it's reasonable to extend this concept of third party processing.*
>
> *It makes sense that the Act would allow an organization to transfer information to a private investigator without consent, in the same way that an organization can transfer personal information to a third party for processing without consent. The private investigator would be acting as the organization's agent. In effect, that means that it is just doing something that the organization itself would be entitled to do under the Act.*

Subsequently, in *Ferenczy* v. *MCI Medical Clinics* (also involving private investigators, here in the context of personal information gathered for medical malpractice litigation), the court stated[41]:

> *On the basis of the plaintiff's argument, [the defendant] might be permitted to take his own video camera and record surveillance evidence in his own defence, but a licensed private investigator could not do so on his behalf if he was being paid to do so. …. One way to avoid this result, and I conclude it is the correct interpretation of [PIPEDA], is to apply the principles of agency. On this analysis it is the defendant in the civil case who is the person collecting the information for his personal use to defend against the allegations brought by the plaintiff. Those whom he employs, or who are employed on his behalf, are merely his agents. …. The defendant through his representatives was employing and paying an investigator, to collect information for him. It is the defendant's purpose and intended use of the information that one should have regard to in determining the applicability of the Act.*

---

[41] *Supra*, footnote 33; see paragraphs 27 and 30.

Treating information transferred for processing as being still under the control of the transferor for PIPEDA purposes, and making the transferor rather than the transferee subject to statutory control, is also supported by a Privacy Commissioner of Canada Fact Sheet in which the following question and answer are given[42]:

> *If my organization (that is subject to B.C. PIPA) contracts out the administration of a customers' awards program to a PIPEDA organization within the same province, how do we know what law applies to the information transfers to and from the contractor?*
>
> *If the contract you have with the awards program administrator specifies that you have control over the customer information, then this practice is subject to the B.C. PIPA. This is true even though the contractor has temporary physical custody of the records; you continue to have informational control. The contracted organization is subject to your privacy rules for the purpose of this account. The awards program administrator is subject to PIPEDA for its own operations and maybe those of other clients.*

Notwithstanding these interpretations, the legal status of transfers of personal information in outsourcing transactions remains less than totally clear.

4. Reform

In considering whether reform is necessary, and if so what reform, it is useful to consider what our objective should be. One formulation would be the following: To provide reasonable protection for the personal information of individuals, while not causing any unnecessary change in the way business is transacted.

As discussed above, some of the current approaches have the potential to unduly affect how business transactions are conducted. In other cases, substantial uncertainty exists regarding the legal basis for the approach.

Any reform has to consider two components: amendments to PIPEDA, and the implementation of a generally-applicable Ontario privacy statute.

a) PIPEDA

(i) Business Transaction Exception

In the absence of generally-applicable privacy legislation in Ontario, PIPEDA governs (other than with respect to personal health information). As well, PIPEDA will in any case govern federally-regulated organizations in Ontario, as well as interprovincial and international transfers into and out of Ontario.

---

[42] *Supra*, footnote 36; see also Privacy Commissioner of Canada Findings, PIPED Act Case Summaries #35, 262 and 269, which seem to accept the concept of transfers to service providers.

Clearer rules for business transactions would enable such transactions to be done more efficiently. As well, this would assist in the establishment of proper practices for handling such transactions, enhancing the protection of the personal information involved.

In respect of business transactions in general, adoption of rules similar to the British Columbia and Alberta rules discussed above in section 3.a)(viii) would provide much more certainty, and would allow a consistent approach for transactions involving those and other jurisdictions. Eventually this should lead to more or less uniform rules across Canada for such transactions.

Some differences exist between the British Columbia and Alberta rules. Specifically, the British Columbia business transaction exception is restricted to the personal information of employees, customers, directors, officers and shareholders only. Personal information of others, such as independent contractor suppliers and service providers, partners, prospective and former employees, and others are not included. Rather than impose these artificial distinctions, it would be better not to restrict the types of personal information in this way, but rather to rely on the other applicable restrictions, e.g. that the information be limited to that which is necessary for the purposes of the transaction.

The British Columbia statute also imposes the requirement that the individuals whose personal information is disclosed be notified that the business transaction has taken place, and that their personal information has been disclosed to the acquirer. This seems to be a reasonable requirement, that would provide an opportunity for individuals to withdraw their consent to ongoing retention and use of their information in the rare cases where they object to the acquirer. This also seems reasonable given that acquirers will usually want or need to notify customers, employees and others that the transaction has taken place.

One issue that has been raised is whether enacting detailed rules regarding business transactions would be within the constitutional power of the federal Parliament. While a discussion of this and other constitutional questions[43] is outside the scope of this paper, query: (i) whether the ability to impose restrictions on transfers of personal information in business transactions might not also imply the ability to create exceptions from such restrictions; and (ii) whether such an exception might not be treated for constitutional purposes in a similar way to the debt collection exception in paragraph 7(3)(b) of PIPEDA.

(ii) Implied Consent

If a business transaction exception as discussed above is provided, it will not be necessary to rely on the concept of implied consent for that purpose. However, the concept of implied consent would be useful for other purposes, and could be usefully imported into PIPEDA.

As discussed above[44], various statutes contain implied consent provisions. However, the Alberta and British Columbia statutes restrict this concept to situations where the individual has

---

[43] In late 2003 the Quebec government initiated a constitutional challenge to PIPEDA.

[44] See footnote 35.

voluntarily provided the information to the organization for the particular purpose in question, but has not provided actual consent. In contrast, the draft Ontario *Privacy of Personal Information Act, 2002*, would have required only that the purpose be reasonably obvious to the individual, and that it be reasonable to expect that the individual would consent to the collection, use or disclosure. This latter approach would appear to provide welcome flexibility for implied consent in circumstances where information is provided for one purpose, but needs to be used for a different but obvious purpose.

(iii) Outsourcing

As discussed above, PIPEDA does not contain express authority for outsourcing. Other statutes approach this issue in different ways. The British Columbia statute expressly provides that an organization may transfer information to another organization if the information was obtained by the transferor with consent, and the information is transferred solely for the purposes for which the information was previously collected, and to assist the transferee to carry out work on behalf of the transferor.[45]

The Alberta statute instead adopts the agency concept, and states that where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with the statute.[46] The *Personal Health Information Protection Act, 2004* (Ontario)[47] and the draft Ontario *Privacy of Personal Information Act, 2002* take a similar approach[48], and expressly indicate that a transfer to an agent is not a disclosure.

In addition, *An Act Respecting the Protection of Personal Information in the Private Sector* (Quebec) adopts the agency approach. Section 20 states:

> *In the carrying on of an enterprise, authorized employees, mandataries or agents may have access to personal information without the consent of the person concerned only if the information is needed for the performance of their duties or the execution of their mandates.*

Some provisions addressing the issue of outsourcing should be included in PIPEDA, to provide for certainty and uniformity across Canada. It is suggested that the agency concept discussed above is more widely used, is more consistent with the outsourcing concept, and should be adopted within PIPEDA.[49]

---

[45] *Personal Information Protection Act* (British Columbia), subsections 12(2), 15(2) and 18(2). Such a transfer is treated in this statute as a disclosure, rather than a transfer for processing.

[46] *Personal Information Protection Act* (Alberta), subsection 5(2).

[47] See sections 2 (definition of "agent"), 6(1), 17 and 37(2).

[48] See sections 2 (definitions of "agent", "collect", "disclose" and "use") and 23.

[49] See also the Gramm-Leach-Bliley Act (U.S.), 15 U.S.C. § 6801-6809, paragraph 6802(b)(2), http://www.ftc.gov/privacy/glbact/index.html, and the concept of "controller" and "processor" in the European Data Directive, *supra*, footnote 5.

(iv) Jurisdictional Issues

As mentioned above[50], the possibility of more than one privacy statute applying to one transaction gives rise to complexity, uncertainty and heightened compliance costs. Although a discussion of this issue is outside the scope of this paper, consideration should be given to amendments to PIPEDA to clarify when it applies.

(v) Process for Change

Section 29 of PIPEDA provides for a review of the statute by Parliament every five years after coming into force. The first such review would be in 2006, and consultations with stakeholders are planned to take place before then. This review process would be an appropriate time to make the changes in PIPEDA discussed above.

b) Ontario

Ontario has tried in the past to put general purpose privacy legislation in place, without success. More recently it has concentrated on the protection of personal health information, resulting in the enactment of the *Personal Health Information Protection Act, 2004* (Ontario). However, no current plans to introduce general privacy legislation have been announced.

Enacting generally-applicable privacy legislation in Ontario would have the advantage of providing a sound constitutional basis for privacy regulation in Ontario, and in particular, would provide welcome clarification of the rules for transfers of personal information in business transactions as discussed in this paper. Ontario legislation would also provide protection for the personal information of employees of provincially-regulated organizations, not now covered by PIPEDA.

If and when a generally-applicable privacy statute is enacted in Ontario, the inclusion of provisions similar to those discussed above for PIPEDA would provide needed consistency and certainty.

5. Conclusion

While approaches to the problem of transfers of personal information in business transactions have evolved, these are not entirely satisfactory. Amendments to PIPEDA and the enactment of similar Ontario general purpose privacy legislation would help to provide a legal framework conducive to business transactions vital to our economy.

---

[50] *Supra*, footnote 36.