mcmillan

employment and labour relations bulletin

December 2008

application of privacy laws to employee information in a sale of business

*Lyndsay Wasser**

"…[L]aw firms have shown a lack of attention to the impact of privacy laws on the myriad legal processes involving the collection, use and disclosure of personal information, including client information and third party information that are common in the type of work they perform on behalf of their clients. Privacy laws are complex, and have implications for their clients on many different types of transactions, including mergers and acquisitions…. We believe that lawyers and law firms require heightened awareness and knowledge of privacy laws in order to properly recognize these implications."[1]

This quote was taken from a 2005 decision of Alberta's Information and Privacy Commissioner in respect of a complaint relating to employee information disclosed in the course of a business transaction.[2] Although Alberta, unlike Ontario, has personal information protection legislation that is directly applicable to employee personal information, this statement could apply equally to employers in Ontario that are (or may be) subject to the Federal *Personal Information Protection and Electronic Documents Act*[3] ("PIPEDA" or the "Act").

Introduction

In recent years both employees and employers have become more aware of, and concerned about, privacy issues. However, Ontario has only enacted provincial privacy legislation dealing with personal health information or information held by public bodies. Further, PIPEDA does not generally apply to employee information that is collected, used or disclosed by provincially-regulated organizations.

Still, one issue that remains to be determined is whether PIPEDA has any application to employee information that is collected, used or disclosed by a provincially regulated employer in connection with a commercial transaction such as a sale of business.

Application of PIPEDA

Under *The Constitution Act, 1867*[4] the federal government has the power to regulate trade and commerce and the provincial governments have jurisdiction over property and civil rights. On this basis, it is clear that the scope of PIPEDA is necessarily limited to commercial matters and not employment matters.

Section 4(1) of PIPEDA provides that the Act applies to every organization in respect of personal information that:

a. the organization collects, uses or discloses in the course of commercial activities; or
b. is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.[5]

It is not clear that the two applications of the Act are mutually exclusive, and on a plain reading there appear to be two reasonable interpretations. The first potential interpretation is that the specific reference to employee information at subsection 4(1)(b) has the effect of carving employee personal information out from subparagraph 4(1)(a) of the Act. If this interpretation is correct, personal information relating to employees of provincially regulated organizations would be excluded from the application of PIPEDA for all purposes.[6]

However, another reasonable interpretation is that subsection 4(1)(b) only applies to collection, use and disclosure of employee information by federal organizations in the context of the employment relationship.[7] Under this interpretation, 4(1)(a) of the Act would apply to all personal information, including employee information, which is collected, used or disclosed by federal and provincial organizations in the course of commercial activities. Thus, PIPEDA could apply to employee information collected, used or disclosed by provincially regulated organizations in the context of a commercial transaction such as a sale of business.[8]

Parliament could have clarified this matter by specifically adding personal information respecting employees of provincially-regulated organizations to the list of excluded areas at section 4(2) of PIPEDA. However, no such explicit exclusion exists in the Act.

Some commentators have suggested that any application of PIPEDA to employee information would be unconstitutional, and therefore, the first interpretation of section 4(1) must be correct.[9] In fact, PIPEDA has already been challenged in Quebec on the basis that it interferes with the province's constitutional competence in matters of civil rights. However, the constitutional reference (which was submitted to the Quebec Court of Appeal in December 2003) has not yet been decided.

Further, there does not appear to be any case law to date that directly addresses whether PIPEDA applies to collection, use or disclosure of employee information by provincial organizations in commercial transactions such as a sale of a business. Although some publications on the website of the Office of the Privacy Commissioner of Canada clearly state that PIPEDA only applies to employee information where the organization is engaged in a federal work, undertaking or business,[10] these publications are not equivalent to binding authority.

Thus, given the ambiguity in the law, it would be prudent for provincially regulated employers in Ontario to understand the requirements of PIPEDA and consider measures to comply with the Act in the course of a sale of business. Further, whether or not such measures are strictly required by law, provincially-regulated employers may find them to be good business practice. In addition, of course, federally-regulated employers in Ontario must comply with PIPEDA in respect of employee information in the course of a sale of business (and at all other times).

Requirements of PIPEDA

Under PIPEDA, the knowledge and consent of an individual is generally required for the collection, use or disclosure of his/her personal information, and individuals are entitled to know the purposes for which their information will be used or disclosed.[11] "Personal information" is broadly defined in PIPEDA as "…information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization".

Consent may be implied, in some circumstances, where the personal information is not "sensitive".[12] However, as indicated further below, the applicability of implied consent to collection, use and disclosure of employee information in the course of a sale of business may not be possible in every case.

Further, unlike its provincial counterparts in Alberta and British Columbia, PIPEDA does not presently have any provisions permitting an organization to disclose personal information to a purchaser or prospective purchasers without consent in the context of a sale of business. In the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics (the "Committee"),[13] the Committee recommended that this be rectified, as follows:

> The Committee recommends that PIPEDA be amended to include a provision permitting organizations to collect, use and disclose personal information without consent, for the purposes of a business transaction. This amendment should be modeled on the Alberta Personal Information Protection Act in conjunction with the enhancements recommended by the Privacy Commissioner of Canada.[14]

The Alberta *Personal Information Protection Act*[15] ("Alberta PIPA") generally provides that personal information (including employee personal information) can be disclosed without consent in the course of a business transaction (including a sale of business), if certain conditions are met. The requirements of Alberta PIPA and the enhancements proposed by the Privacy Commissioner of Canada are discussed further below.

In its response to the Fourth Report of the Committee, the government of Canada agreed with this recommendation of the Committee and acknowledged that it reflects a "general consensus" that PIPEDA should be modified to allow collection, use and disclosure of personal information without consent in the course of business transactions.[16] However, PIPEDA has not yet been amended and the government has indicated that it intends to conduct further consultations on the Committee's recommendations.

Strategies for Compliance

There are two stages where employee information may be collected, used or disclosed in the context of a sale of business: (1) the "due diligence" phase, when the vendor provides information to a purchaser or prospective purchasers for the purposes of allowing such persons to evaluate the business; and (2) on closing of the sale, when the business is transferred to the purchaser.

Both vendors and potential purchasers should be cognizant of PIPEDA at both stages of a sale of business, since the Act potentially applies to both parties' collection, use and disclosure of personal information. Some strategies for compliance include:

1. *Limit personal information transfers*. Only information that is necessary for purchasers to evaluate the business and complete the transaction should be disclosed. In one case, the Alberta Information and Privacy Commissioner (the "Commissioner") found that, although what is necessary is a factual inquiry, disclosure of employee home addresses and Social Insurance numbers was not necessary in the due diligence phase of a transaction. The Commissioner further suggested that it may be necessary to disclose the following types of employee information:[17]
    a. names, titles, positions and functions;
    b. employee's place in the target's management structure;
    c. outstanding employee litigation;
    d. membership in benefit plans, pension plans, stock purchase plans and/or collective bargaining units; and
    e. salary levels (in some cases).
2. *Provide aggregate or de-identified information at the due diligence phase*. If individuals cannot be identified from the information, then the information is not considered to be "personal information" under PIPEDA and consent to disclosure is not required. However, in some cases individuals may be identifiable even if aggregate information is provided or names are removed (e.g., in smaller companies).
3. *Obtain consent*. Depending upon the commercial sensitivity of the transaction, it may be possible to obtain consent from some or all employees. In an asset sale, on closing, the purchaser can include a request for consent to transfer employees' personal information in its employment offer letters.[18] In the due diligence phase, requests for consent may be limited to certain key employees, if the purchaser requires specific personal information about such persons (or they are likely to be identifiable even in aggregate or de-identified data).
4. *Rely on prior consent*. In some cases, employers obtain consent to the collection, use and disclosure of employee information at the time of hiring, or in the course of the employment relationship. This may be included in an employment contract or the employer's privacy policies. However, the language of such consent must be examined to determine if it is broad enough to cover: (a) collection, use and disclosure of personal information for the purpose of a sale of business; and (b) the personal information that will be transferred to potential purchasers.[19]

5. *Rely upon implied consent*. The question of whether there can be implied consent to disclose employee information in the context of a sale of business has not yet been considered by the Federal Privacy Commissioner. In part, this determination will likely be a factual matter that is dependent upon the reasonable expectations of employees as well as the sensitivity of the information transferred.[20]

Although not required, Ontario employers may also chose to adopt an approach similar to that required in Alberta PIPA and British Columbia's *Personal Information Protection Act*[21] ("BC PIPA") as well as the "enhancements" recommended by the Federal Privacy Commissioner. This is a comprehensive approach that covers both the due diligence stage of a transaction, as well as transfers of personal information upon closing. The requirements of Alberta PIPA and BC PIPA, together with the enhancements recommended by the Federal Privacy Commissioner, include the following:

a. During the due diligence phase:
    i. an agreement between the parties, which provides that the personal information will only be collected, used and disclosed for purposes related to the business transaction;
    ii. only information that is necessary for the parties to determine whether to proceed with the transaction, and then to carry out the transaction, can be transferred; and
    iii. the information that is transferred must be the least amount of personally identifiable information possible.[22]
b. On and after closing:
    i. an agreement between the parties that personal information will only be used or disclosed for the purposes that it was originally collected;
    ii. only information that is necessary for carrying on business can be transferred;
    iii. after a transfer of ownership, all employees whose information has been transferred without consent should be notified as soon as possible; and
    iv. the new employer must adhere to the vendor's employee privacy policies until employees have an opportunity to choose whether they want to continue their relationship with the new employer.
c. If the transaction does not proceed, the personal information must be returned to the vendor or destroyed.[23]

Organizations that are subject to PIPEDA, which adopt this approach, will likely find themselves in a good position if PIPEDA is eventually amended to reflect the Committee's recommendations for reform of the Act.

Additional Considerations

In every transaction there is the potential for additional issues to arise. For instance, provincial privacy laws in Alberta, British Columbia and/or Quebec may need to be considered if the organization has employees in those provinces, or if a prospective purchaser is located in one of those provinces. In particular, this may complicate the transaction if employees or potential purchasers are located in Quebec, since Quebec privacy legislation does not contain special provisions for business transactions.

Further, other complications may arise if the prospective purchaser is located in another country and personal information will be communicated outside Canada in the course of the transaction. Other countries may have their own privacy law, which may need to be taken into consideration. In addition, if the information will be communicated to persons located in the United States, the impact of the *Patriot Act*[24] may need to be considered.

Further, if the workforce is unionized, the collective agreement should be examined to determine if such agreement contains any relevant provisions dealing with employee privacy rights.

As indicated in the quote from the Alberta Privacy Commissioner first set out above, privacy laws are complex and have implications for many different types of transactions. However, the first step for employers is to attain a heightened awareness of privacy laws and potential compliance strategies.

**Lyndsay Wasser is an associate in the Employment and Labour Relations Group of McMillan LLP.*

This article originally appeared in the OBA Privacy Law Review, Eye on Privacy, Volume 9, No. 1., December 2008.

ENDNOTES

1 Alberta Information and Privacy Commissioner, Investigation Report P2005-IR-005, "Report of an Investigation into the Disclosure of Personal Information During the Course of a Business Transaction" (12 July 2005) at para. 57.

2 In this case, all parties were found to be accountable for breaches of Alberta's privacy legislation, including the vendor, the purchaser and counsel to each of them (although the Commissioner found that the vendor and the purchaser showed some diligence in relying upon their legal counsel).

3 S.C. 2000, c. 5.

4 (U.K.), 30 & 31Vict., c. 3.

5 *Supra* note 4 at s. 4(1).

6 Jeffrey A. Kaufman, *Private Law in the Private Sector: An Annotation of the Legislation in Canada*, vol. 1 (Aurora, ON: Canada Law Book, 2007) at PIP-32.

7 Employment purposes would likely include employee information that is collected, used and disclosed for the purpose of establishing, managing and terminating the employment relationship.

8 *Ibid*. See also Stephanie Perrin *et al.*, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law Inc., 2001).

9 See e.g. Colin H.H. McNairn & Alexander K. Scott, *A Guide to the Personal Information Protection and Electronic Documents Act*, 2008 ed. (Toronto, ON: LexisNexis Canada Inc., 2007) at 21-22.

10 See e.g. *Fact Sheet: Application of the Personal Information Protection and Electronic Documents Act to Employee Records*, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/fs-fi/02_05_d_18_e.asp>; and (2) F*act Sheet: Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts (PIPAs)*, online: Office of the Privacy Commissioner of Canada. <http://www.privcom.gc.ca/fs-fi/02_05_d_18_e.asp>.

11 The consent requirements are subject to specified exceptions, which are not applicable to the present analysis.

[12] *Supra* note 4 at Schedule 1, clause 4.3.6. See also *PIPEDA Case Summary* #351, 2006 CarswellNat 5577 (Can. Privacy Commr.) (WLeC).

[13] The Committee's 2006/2007 review of PIPEDA was undertaken pursuant to section 29 of PIPEDA, which requires a review of Part 1 of the Act every five years, and an order of the House of Commons.

[14] "Fourth Report of the Standing Committee on Access to Information Privacy and Ethics" (39th Parliament, 1st Session), Chairman Tom Wappel, MP, May 2007, Recommendation 7.

[15] S.A. 2003, c. P-6.5.

[16] Canada, "Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics" (Statutory Review of the *Personal Information Protection and Electronic Documents Act* PIPEDA) (17 October 2007) at 5. Available online: <http://www.ic.gc.ca/epic/site/ic1.nsf/en/00317e.html>.

[17] *Supra* note 2 at para. 28.

[18] In a share sale, generally, the same corporate entity will hold employee personal information before and after the transaction, and therefore, disclosure of information will not be required upon closing.

[19] Some commentators have questioned whether vague consents, that do not identify the purchaser or the date of a transaction, would be effective. See e.g. Jenifer E. Aitken, "Avoiding Privacy Pitfalls in Business Transactions No Easy Task", *The Lawyers Weekly* (12 December 2003).

[20] *Supra* note 4 at Schedule 1, clause 4.3.6. See also *PIPEDA Case Summary* #351, 2006 CarswellNat 5577 (Can. Privacy Commr.) (WLeC).

[21] S.B.C. 2003, c. 63.

[22] BC PIPA further requires that disclosure be limited to personal information that relates directly to the part of the business that is covered by the transaction.

[23] *Supra* note 15, at 16-18.

[24] Pub L. No. 107-56, 115 Stat. 272 (2001).

For more information, contact any of the lawyers listed below:

Calgary	Michael A. Thackray, QC	403.531.4710	michael.thackray@mcmillan.ca
Toronto	David Elenbaas	416.865.7232	david.elenbaas@mcmillan.ca
Montréal	Dino Mazzone	514.987.5011	dino.mazzone@mcmillan.ca

a cautionary note