CANADIAN PRIVACY LAWS AND INTERNATIONAL TRANSACTIONS

By: Paige Backman[1]

The *Personal Information Protection and Electronic Documents Act* ("***PIPEDA***"), together with a few select pieces of provincial legislation,[2] (collectively, "**Canadian Privacy Legislation**") govern the collection, use, and disclosure of personal information held by private sector organizations. Canadian Privacy Legislation can have a significant impact on cross border business transactions involving personal information assets ("**PIA**"). The impact of Canadian Privacy Legislation on cross-border business transactions can be broken down in four general areas: (i) pre-transaction due diligence and investigations; (ii) the structuring of the transaction; (iii) transaction specific issues such as purchase price, and representations, warranties and indemnities negotiated between the parties; and (iv) post-closing issues. While the majority of this article focuses on the impact of *PIPEDA* on pre-transaction due diligence and investigations that arise in the context of a merger, acquisition, or amalgamation of a Canadian organization by a foreign entity, a brief discussion of the impact of *PIPEDA* on the three remaining areas is also included.

(a) Pre-Transaction Due Diligence and Investigations

Prior to the disclosure of any personal information to a purchaser or third party, including advisors, the parties first need to determine: (i) what Canadian federal and provincial privacy laws affect the target business; (ii) any industry specific or other privacy policies and codes the target business is obligated or with which it has voluntarily chosen to comply; and, (iii) any contractual obligations the target must adhere. To make this determination, one must not only understand the Canadian Privacy Legislation applicable to the specific instance, but also review internal privacy policies, privacy policies circulated externally to customers and third-party service providers, and privacy policies pertaining to the collection of personal information on-line and posted on the business' website.[3]

In addition to the foregoing, the parties must consider:

1) How personal information held by the target business was acquired, whether appropriate consents were obtained for the current use, and for the use the acquirer intends to make of the personal information post-transaction, and whether there exists contractual obligations and restriction pertaining to the collection, use, and disclosure of the personal information;

2) If third-party service providers (e.g. information management companies) have access to personal information held by the target company, whether there are sufficient contractual provisions in place to ensure the security of such information and whether such third parties are in compliance with the relevant contractual provisions;

3) Whether there are any encumbrances on the business that could affect PIA, including whether PIA have been put up as security for financing; and[4]

4) Whether there are, or have been, any complaints, or incidences that could result in a complaint, that have been made regarding the handling of the personal information.

Without completing the foregoing pre-transaction due diligence, the purchaser will not be aware of (i) what PIA can be transferred to the purchaser; (ii) what consents, if any, will have to be obtained; (iii) what, and with whom, PIA can be shared; and (iv) what restrictions must be placed on any of the foregoing areas of disclosure, and any subsequent use of the desired PIA, by the purchaser.

Provincial private sector privacy laws, can add additional elements to the pre-transaction considerations. Alberta and British Columbia's private sector privacy legislation, both entitled the *Personal Information Protection Act* ("***PIPA***") place further limitations on what information can be disclosed to a purchaser during the pre-transactional due diligence stages of a business transaction, and require the purchaser and target business to enter into a 'confidentiality' agreement prior to any such disclosure.

(b) Structure of the Transaction

Where the resources required to obtain the requisite consents from individuals to whom the PIA being purchased relates are substantial, a share purchase or debt financing with options for shares, as opposed to a direct purchase of the PIA, may be a more appropriate structure for the transaction as the purchaser would arguably not need to obtain the consent of the individuals to whom the PIA relates.[5]

However, utilizing a share purchase is not without issues.[6] Contracts containing 'change of control' provisions would still require the consents of the individuals to whom the desired PIA relate. Further, as with all share purchases, the purchaser would be assuming the target business' liabilities associated with the mishandling of the PIA (in addition to all other non-PIA liabilities).

There are potentially other business structures available to manage and limit the risk associated with 'unclean' PIA.

(c) Transaction Specific

Once the structure of the deal is settled, the parties will need to address a number of transaction specific issues. First, the parties will have to attribute a value to the PIA by taking into account the results from the due diligence discussed above. Second, the parties will have to determine what consents, if any, need to be obtained and how such consents will be acquired. Thirdly, the parties will need to determine the representations, warranties, and indemnities that will be included in the agreement. Finally, the parties will need to determine what, if any, public disclosure will be required concerning the acquisition of the PIA; specifically, where one or both of the parties is a public company there may be obligations to disclose the risks involved in purchasing or selling the PIA in public disclosure documents.

(d) Post-Transaction Issues

Once the transaction is complete, the purchasing company will need to address: (i) legal requirements to notify individuals on whom personal information was transferred that the transaction has taken place and that their personal information has been disclosed[7]; (ii) which privacy policies and procedures will govern the PIA; (iii) the training of employees (both old and new) regarding such privacy policies; (iv) the appointment of a chief privacy officer or the equivalent; and (v) the dissemination of any new privacy policies and privacy officer contact information to all individuals, employees, and third parties to whom the PIA relate or who may come in contact with such PIA.

CONCLUSION:

The application of *PIPEDA* to foreign entities wishing to acquire a Canadian organization can be significant and requires careful consideration. This article has attempted to illustrate some of the issues foreign entities must address both during and after the transaction. In addition to the foregoing, foreign entities must also be aware of two potentially dangerous pitfalls that face foreign entities operating in Canada.

For more information on this topic, or any other legal topic relating to corporate or technology law, please do not hesitate to contact the author, Paige Backman, at 416.865.7700 or pbackman@airdberlis.com.

[1] Assistance of Matthew Kindree and Adrian Liu, students of law at Aird & Berlis LLP, acknowledged with gratitude.

[2] This article focuses primarily on the impact of *PIPEDA* on international business transactions and discusses briefly the impact of British Columbia's *Personal Information Protection Act*, S.B.C. 2003 c. 63 and Alberta's *Personal Information Protection Act*, S.A. 2003, c. P-6.5; however, as of the date of writing this article, there are a number of other provincial private sector privacy statutes that must be considered when contemplating a business transaction. Quebec has enacted the *Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1, and Ontario has enacted the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3.

[3] It is important to note that, notwithstanding an organization may not legally be required to have a privacy policy, if the organization in fact suggests to the public that it does have a policy dealing with the handling of personal information and the organization does not adhere to it, the business may be subject to legal claims of, among other things, misleading advertising which can exact substantial penalties.

[4] The purchaser may wish to have such encumbrances discharged prior to completion of the business transaction or may wish to reduce the purchase price for the business (or the PIA) accordingly.

[5] This assumes that the PIA would be used in the same manner and for the same purposes after the transaction as they were before the transaction.

[6] Other possible methods of structuring the transaction might include (i) rolling the PIA into a wholly owned 'shell company' subsidiary of the target company to isolate the liabilities associated with the PIA; (ii) effecting a purchase of assets not including the PIA; or (iii) insisting the PIA be sold off or destroyed prior to completing the share purchase.

[7] For example, British Columbia's *PIPA* places conditions on the disclosure of personal information once the transaction is complete, including a requirement that the parties notify the individuals about whom the personal information relates that the transaction has taken place and that their personal information has been disclosed.