mcmillan

Cybersecurity Bulletin

April 2016

Privacy and Cybersecurity Issues in Canadian M&A Transactions[1]

Privacy and cybersecurity have become areas of significant potential liability in Canada and elsewhere. Organizations that misuse personal information or fall victim to a data breach face reputational damage, regulatory scrutiny and possible class action lawsuits. In addition, businesses that fail to comply with "Canada's Anti-Spam Law"[2] ("CASL") can be subject to significant fines.

In the context of M&A transactions, it is important for organizations to understand applicable statutory requirements and take steps to reduce and mitigate risks. This will involve consideration of privacy and cybersecurity issues in the due diligence process and negotiation of the purchase agreement, as well as attention to restrictions upon transfer and use of personal information on and after closing.

---

[1] This article will focus on private sector laws. Most jurisdictions in Canada also have public sector privacy laws, as well as specific legislation applicable to collection, use, protection and disclosure of personal health information.

[2] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the *Canadian Radio-television and Telecommunications Commission Act*, the *Competition Act*, the *Personal Information Protection and Electronic Documents Act* and the *Telecommunications Act*, S.C. 2010, c. 23.

Due Diligence

In order to determine the amount and extent of privacy and cybersecurity due diligence that will need to be performed in a transaction, it is important to initially consider the nature of the target's business. Some businesses, like traditional manufacturing companies, may process minimal sensitive or personal information. Therefore, it may be unreasonable to expect that such organizations would have detailed and comprehensive privacy compliance infrastructures, and risks related to privacy and cybersecurity may be limited. In such cases, the scope of due diligence with respect to privacy and cybersecurity matters could be fairly narrow.

However, in this "information age" the core function of many businesses revolves around data. When organizations seek to purchase these types of businesses, it is important to thoroughly canvas the target's history and current practices and procedures, to identify any potentially significant liabilities. Poor information handling practices or outdated technological controls may require a significant investment to bring the business into compliance with all applicable laws, or in a worst case scenario could expose the business to costly litigation.

In each case, the documents and information requested in the due diligence process will vary depending upon the circumstances. In particular, pursuant to changes made to Canada's Federal privacy law - the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") - in 2015, personal information[3] can only be disclosed in the context of a prospective business transaction without the knowledge and consent of affected individuals, if: "*…the personal information is necessary to determine whether to proceed with the transaction, and if the determination is made to proceed with the transaction, to complete it*."[4] Similar restrictions exist under

[3] Personal information is information about an identifiable individual. It does not include other types of information that may be confidential or proprietary.

[4] PIPEDA s. 7.2(1).

substantially similar legislation in the provinces of Alberta and British Columbia.[5] Therefore, broad and indiscriminate requests for personal information in the due diligence process are not permitted under PIPEDA. Rather, the parties should exchange only the minimum amount of personal information that is required in the circumstances. For example, if aggregate statistics would provide sufficient information to the purchaser, information about identifiable individuals should not be disclosed.

Although an individualized approach is necessary, some examples of information and documents that may be requested in connection with privacy and cybersecurity due diligence include:

- Copies of privacy, data security and CASL policies and procedures, including but not limited to breach response plans as well as cybersecurity governance and risk procedures;
- Information about privacy and cybersecurity audits, including how often they are conducted and copies of recent reports;
- Information about the target's process for obtaining, recording and giving effect to withdrawal of consent (i.e., CASL consents as well as consents under PIPEDA and substantially similar provincial legislation), including copies of standard consent forms;
- Information respecting training of employees on privacy and cybersecurity compliance, as well as copies of any agreements with employees related to such matters;
- Information on any significant or recent breaches, including privacy, data security, cybersecurity and CASL breaches, as well as any actual or threatened claims, complaints, litigation or regulatory action related to such breaches;
- Information respecting the vendor/service provider selection and management process, including selection policies and procedures, copies of vendor privacy and data security questionnaires, and

[5] Quebec privacy legislation still technically requires consent for any disclosure of personal information.

copies of all contracts governing privacy commitments, data protection and CASL compliance (e.g., data sharing agreements or relevant provisions in service agreements); and

- Copies of any cybersecurity insurance policies.

Overall, through the due diligence process, the goal is to gain an understanding of the target company's process for collecting, using, storing, protecting and disclosing personal and other sensitive information. This will allow the purchaser to evaluate legal compliance and identify risks. In addition, in some cases it may be necessary for the purchaser to engage information technology experts (internal or external) in the due diligence process to evaluate the target's cybersecurity controls.

The Purchase Agreement

PIPEDA and substantially similar legislation in Alberta and British Columbia contain specific requirements for the agreement between the parties when personal information will be disclosed in the due diligence process or upon closing of a transaction. For example, under PIPEDA:[6] [7]

> 7.2(1) …[O]rganizations that are parties to a prospective business transaction may use and disclose personal information without the knowledge or consent of the individual if the organizations have entered into an agreement that requires the organization that receives the personal information (i) to use and disclose that information solely for purposes related to the transaction, (ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and (iii) if the transaction does not proceed, to return that information to the organization that disclosed it, or destroy it, within a reasonable time.

[6] PIPEDA s. 7.2(1) and 7.2(2).

[7] It is important to note that: PIPEDA 7.2(1) and (2) do not apply to a business transaction of which the primary purpose or result is the purchase, sale or other acquisition or disposition, or lease, of personal information.

> 7.2(2) …[O]rganizations that are parties to the transaction may use and disclose personal information, which was disclosed under subsection (1), without the knowledge or consent of the individual if the organizations have entered into an agreement that requires each of them (i) to use and disclose the personal information under its control solely for the purposes for which the personal information was collected, permitted to be used or disclosed before the transaction was completed, (ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and (iii) to give effect to any withdrawal of consent made under clause 4.3.8 of Schedule 1.

In addition to these specific statutory requirements, there are a number of privacy and cybersecurity issues that may need to be addressed in a purchase agreement. Again, in each case the specific circumstances and nature of the target's business will need to be taken into account to assess what provisions are appropriate. However, from the purchaser's perspective, it will often be necessary to include representations and warranties addressing the following:

- Compliance with applicable laws and the seller's own privacy, data security, cybersecurity and CASL policies and procedures (and that the target's policies, procedures, and practices meet or exceed industry standards);
- Compliance with all privacy, data protection and CASL requirements under contracts with customers and other third parties (and that the target is not aware of any non-compliance with contractual obligations of its own service providers);
- Training of employees on privacy, data security, reporting and responding to data breaches, and CASL compliance (and in some cases that employees are subject to appropriate contractual obligations);
- Sufficiency of data security and cybersecurity controls, including that the organizational, technological and physical security measures are reasonable in relation to the sensitivity of the information collected and held by the organization; and

- Disclosure of any material or recent privacy, data security, cybersecurity and CASL breaches, or confirmation that the seller is not aware of any such breaches.

From the seller's perspective, it may be necessary to limit or qualify some of the representations and warranties described above, by including materiality thresholds or adding knowledge qualifiers that take into account the size and structure of the organization. Most information technology and cybersecurity experts agree that many organizations are not aware of data breaches until months (or years) after they occur. Therefore, the seller will need to carefully consider what representations and warranties can realistically be provided, without risking exposure to potentially significant liability if a pre-closing breach is discovered after completion of the transaction. Also, before giving representations respecting compliance with applicable laws, sellers will need to make sure that they are, in fact, familiar with relevant legal requirements.

Other issues that may need to be considered in connection with the purchase agreement include:

1. ***Purchase price adjustments and holdbacks*** – If due diligence identifies significant risks or vulnerabilities that may impact the value of the target, and if: (a) substantial resources will be required to bring the company into compliance with applicable laws or fix weaknesses in systems that are outdated or have been compromised; or (b) the target has experienced a privacy or cybersecurity breach that has not yet resulted in litigation or other liability, but applicable limitation periods have not yet expired.

2. ***Indemnities*** – Although often covered by general indemnities, specific privacy and cybersecurity indemnities may be warranted in some cases. For example, stand-alone indemnities may be necessary if specific concerns are identified in the due diligence process, or if: (a) the duration of general indemnities is not long enough to take into account the typical delay in identifying data breaches; (b) the cap on general indemnities is too low to

adequately cover the risk of a major cyber breach; or (c) the general indemnities do not protect all relevant parties, such as directors who may be held liable in their personal capacities.

If holdbacks or indemnities are included in the purchase agreement, it is prudent for the parties to include specific mechanisms for the purchaser to claim them, including provisions addressing how damages will be calculated and by whom. Such mechanisms can decrease the chances of future disputes.

Closing and Beyond

After the transaction is completed, the purchaser will, of course, want to benefit from the personal information that was collected by the business pre-closing. However, statutory requirements must be taken into account. For example, under PIPEDA, the parties can only use and disclose personal information that was disclosed in connection with the transaction without obtaining consent from affected individuals, if:[8]

- The personal information is necessary for carrying on the business or activity that was the object of the transaction; and
- One of the parties notifies individuals, within a reasonable time after the transaction is completed, that the transaction has been completed and that their personal information has been disclosed.

The purchaser must also be careful not to use personal information obtained by the target prior to the transaction for purposes other than those encompassed by the consent obtained at the time of collection. In addition, as outlined previously, PIPEDA requires that the agreement between the parties specifically provide that they will give effect to any withdrawal of consent after individuals are notified that their personal information has been disclosed.

Conclusion

[8] PIPEDA s. 7.2(2).

Privacy, data protection and cybersecurity have been the focus of a lot of attention in recent years. The legal framework is complex, and the common law is rapidly developing. Although this is an evolving area, it is clear that privacy and cybersecurity breaches can give rise to significant potential liabilities. Therefore, parties to a prospective business transaction would be well advised to consider and address these issues before, on and after closing.

by Lyndsay Wasser, Co-Chair Cybersecurity

For more information on this topic, please contact:

Toronto Lyndsay A. Wasser 416.865.7083 lyndsay.wasser@mcmillan.ca

a cautionary note