PRIVACY, TECHNOLOGY AND CYBERSECURITY ISSUES IN TECH TRANSACTIONS

Posted on December 6, 2022

Categories: Insights, Publications

With few exceptions, software and information technology systems (collectively, "**IT**") are now integral to most businesses. As a result, an increasing number of transactions involve technology companies ("**Tech Transactions**"), whether they are large IT providers, "tech start-ups" that have attracted the attention of buyers or investors, or even companies that traditionally focused on selling physical products but now use IT to generate revenue through the collection, analysis and/or monetization of data.

As technology permeates more businesses, and the collection, use, sharing and other processing of data becomes increasingly pervasive, privacy, technology and cybersecurity have become areas of significant potential liability in Canada. For example:

- Organizations can face administrative monetary penalties ("**AMPs**") of up to $10 million under the *Competition Act* for false or misleading privacy representations;[1]
- Effective September 2023, Quebec's *Act respecting the protection of personal information in the private sector* (the "**Quebec Act**") will provide for AMPs for non-compliant organizations up to the greater of $10 million or 2% of worldwide turnover for the preceding fiscal year, and fines for certain offences up to the greater of $25 million or 4% of worldwide turnover;
- The federal government has tabled the *Consumer Privacy Protection Act*, which (if passed) would substantially replace the current *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), and provide for AMPs up to the greater of $10 million or 3% of worldwide turnover for the preceding fiscal year, and fines for certain indictable offences up to the greater of $25 million or 5% of worldwide turnover; and
- Data breaches routinely give rise to expensive class action litigation, and reputational harm caused by the erosion of customers' or business partners' trust and/or adverse media attention.

Accordingly, it is important for potential purchasers in Tech Transactions to fully evaluate the target company's privacy, technology and cybersecurity compliance in the diligence phase of the transaction, and for each of the parties to ensure that risks and liabilities are appropriately allocated in the purchase agreement.

Due Diligence

Organizations seeking to purchase a technology-focused business should thoroughly canvas the target's history and current practices and procedures with respect to privacy, technology and cybersecurity. Poor personal information ("**PI**") handling practices, outdated or unsupported IT, or inadequate information security controls may require a significant investment to bring the target into compliance with relevant laws, and give rise to the aforementioned financial and reputational risks.

The documents and information requested in the diligence process will vary depending upon the circumstances. Often, technology diligence may be performed by the purchaser's technical personnel or external consultants while the corresponding legal review is conducted. Examples of materials that may be requested in connection with privacy, technology and cybersecurity diligence include:

- A list of all IT owned or used by the target, identifying proprietary and third party IT, and copies of licenses and other agreements relating to the target's use of third party IT;
- A description of the PI the target collects, holds or otherwise processes in the course of its business;
- Copies of privacy, data security and IT policies and procedures, including (without limitation) breach response and disaster recovery plans, vendor and service provider selection and management procedures, and cybersecurity governance and risk procedures;
- Information about privacy and cybersecurity audits, including frequency, copies of recent reports, and remedial actions taken to address any identified issues;
- Information relating to, or measuring, the effectiveness, security, availability, or integrity of the target's IT;
- Information about the target's process for obtaining, recording and giving effect to consents (and withdrawals of such consents), including copies of the target's privacy notices and consent forms;
- Information about the security measures used by the target to protect IT and safeguard PI;
- Information respecting employee training on privacy and cybersecurity compliance, and copies of any relevant agreements with personnel;
- Information about any significant or recent privacy or cybersecurity breaches ("**Breaches**");
- Information on any actual or threatened claims, complaints, litigation or regulatory action related to privacy or data security;
- Copies of all contracts containing privacy and data protection terms (e.g., data sharing agreements or relevant provisions in service agreements); and
- Copies of any cybersecurity insurance policies.

Overall, through the diligence process, the goal is to gain an understanding of: (1) the target's process for collecting, using, storing, protecting and disclosing personal and other sensitive information, and (2) the

performance levels, adequacy, suitability and scalability of the target's IT in view of the target's business and business plans. Such understanding will allow the purchaser to evaluate legal compliance and identify risks and potential liabilities.

Sharing Personal Information

While it may be necessary for certain PI to be disclosed by the target to the purchaser during the due diligence process, organizations must consider the potential limits on doing so.

For example, pursuant to PIPEDA, PI can only be disclosed in the context of a prospective business transaction without the knowledge and consent of affected individuals if such information is necessary to determine whether to proceed with the transaction, and, if the determination is made to proceed, to complete it.[2] Similar restrictions exist under private sector privacy legislation in Alberta[3], British Columbia[4] and Quebec[5] (the "**Provincial Legislation**").

Therefore, broad and indiscriminate requests for and disclosure of PI in the diligence process are not permitted under Canadian privacy laws. Rather, the parties should exchange the minimum amount of PI 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.

PIPEDA and the Provincial Legislation[6] also contain specific requirements for the parties to enter into an agreement when PI will be disclosed in the due diligence process. For example, under PIPEDA[7], parties to a prospective business transaction may use and disclose PI without the knowledge or consent of individuals if they have entered into an agreement that requires the recipient: (i) to use and disclose the PI solely for purposes related to the transaction, (ii) to protect the PI by security safeguards appropriate to the sensitivity of the PI, and (iii) if the transaction does not proceed, to return or destroy the PI within a reasonable time. In practice, these terms can be incorporated into a broader non-disclosure or confidentiality agreement that the parties sign at the outset of the due diligence process.

Purchase Agreement

There are a number of privacy, technology and cybersecurity issues that may need to be addressed in a purchase agreement (the "**Agreement**"). For example, the purchaser may want to include representations and warranties ("**Reps & Warranties**") addressing the following:

- Compliance with applicable laws and the target's own privacy, information technology and cybersecurity policies and procedures, and confirmation that such policies, procedures, and practices meet or exceed industry standards;
- Compliance with all privacy, data protection and cybersecurity requirements under contracts with third

parties;

- Sufficiency of IT owned or used by the target in meeting its data processing and other computing needs;
- Training of employees on privacy and data security, and that employees are subject to appropriate contractual obligations;
- Accuracy of the target's external-facing privacy policies, notices and representations;
- Sufficiency of data security controls, including that the organizational, technological and physical security measures are reasonable in relation to the sensitivity of the PI processed by the target; and
- Disclosure of all Breaches, as well as malfunctions, defects, technical concerns and failures related to IT owned or used by the target, and confirmation that all of the foregoing have been remedied.

From the target's perspective, it may be necessary to limit or qualify some Reps & Warranties, by including materiality thresholds or adding appropriate knowledge qualifiers. The target will need to carefully consider what Reps & 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, the target will need to ensure it is familiar with relevant legal requirements and all IT that it owns or uses before making certain Reps & Warranties.

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

1. ***Purchase price adjustments and holdbacks*** – A purchase price adjustment and/or holdback may be warranted if due diligence identifies significant risks or vulnerabilities that may impact the target's value, and: (a) substantial resources will be required to bring the target into compliance with applicable laws or to fix outdated or compromised IT; or (b) the target has experienced a 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 Breaches; or (b) the cap on general indemnities is too low to adequately cover the risk of a major Breach.

To decrease the chances of future disputes regarding any holdbacks or indemnities included in the Agreement, it is prudent for the parties to include specific mechanisms for the purchaser to make a claim against them, including provisions addressing how damages will be calculated and by whom.

Closing and Beyond

After the Tech Transaction is completed, the purchaser may want to consider whether the existing IT is

sufficient to accomplish its plans for the purchased business. Any deficiencies regarding IT discovered during the due diligence process should be addressed promptly to align with the purchaser's plans for the business.

With respect to the post-closing processing of PI collected by the business pre-closing, statutory requirements must be taken into account. For example, under PIPEDA, the parties can only use and disclose PI that was disclosed in connection with the transaction without obtaining consent from affected individuals, if:[8]

- The PI 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 PI has been disclosed.

Similar obligations exist under the Provincial Legislation.[9] Accordingly, the purchaser must not use PI obtained by the target prior to the transaction for purposes other than those permitted by applicable law and covered by existing consents (where applicable). In addition, as outlined previously, PIPEDA requires that an agreement between the parties specifically provide that they will give effect to any withdrawal of consent after individuals are notified that their PI has been disclosed in connection with the transaction.

Conclusion

The legal framework around privacy, data protection, technology and cybersecurity is complex, and the common law is rapidly developing. Although these are evolving areas, it is clear that poor PI handling practices and mismanaged IT can have a significant impact on a business, and also expose it to material costs and liabilities. Therefore, parties to Tech Transactions should consider and address these issues before, on and after closing of the deal.

[1] See seminal 2020 case at: https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/471812/index.do.
[2] PIPEDA s. 7.2(1)(b). Note: Section 7.2(1) of PIPEDA does 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 PI.
[3] *Personal Information Protection Act* (Alberta) ("**Alberta PIPA**") s. 22(3)(a)(ii). Note: Section 22 of Alberta PIPA does not apply to a business transaction where the primary purpose, objective or result of the transaction is the purchase, sale, lease, transfer, disposal or disclosure of PI.
[4] *Personal Information Protection Act* (British Columbia) ("**B.C. PIPA**") s. 20(2)(a). Note: Section 20 of B.C. PIPA does not authorize an organization to disclose PI to a party or prospective party for purposes of a business transaction that does not involve substantial assets of the organization other than this PI.
[5] Effective September 2023, s. 18.4 of the Quebec Act will provided that: "Where the communication of personal information is necessary for concluding a commercial transaction to which a person carrying on an enterprise intends to be a party, the person may communicate such information, without the consent of the

person concerned, to the other party to the transaction." (emphasis added).
[6] Alberta PIPA s. 22(3)(a)(i); B.C. PIPA s. 20(1)(b). Effective September 2023, s. 18.4 of the Quebec Act will require that the agreement must stipulate, among other things, that the recipient of the personal information undertakes: "(1) to use the information only for concluding the commercial transaction; (2) not to communicate the information without the consent of the person concerned, unless authorized to do so by this Act; (3) to take the measures required to protect the confidentiality of the information; and (4) to destroy the information if the commercial transaction is not concluded or if using the information is no longer necessary for concluding the commercial transaction."
[7] PIPEDA s. 7.2(1)(a). Note: Section 7.2(2) of PIPEDA does 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 PI.
[8] PIPEDA s. 7.2(2).
[9] Alberta PIPA s. 22(3)(b); B.C. PIPA s. 20(3). Effective September 2023, s. 18.4 of the Quebec Act will provide that: "[w]here the commercial transaction has been concluded and the other party wishes to continue using the information or to communicate it, that party may use or communicate it only in accordance with this Act. Within a reasonable time after the commercial transaction is concluded, that party must notify the person concerned that it now holds personal information concerning him because of the transaction."

by Lyndsay Wasser, Robert Piasentin, Kristen Pennington, and Yue Fei

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.