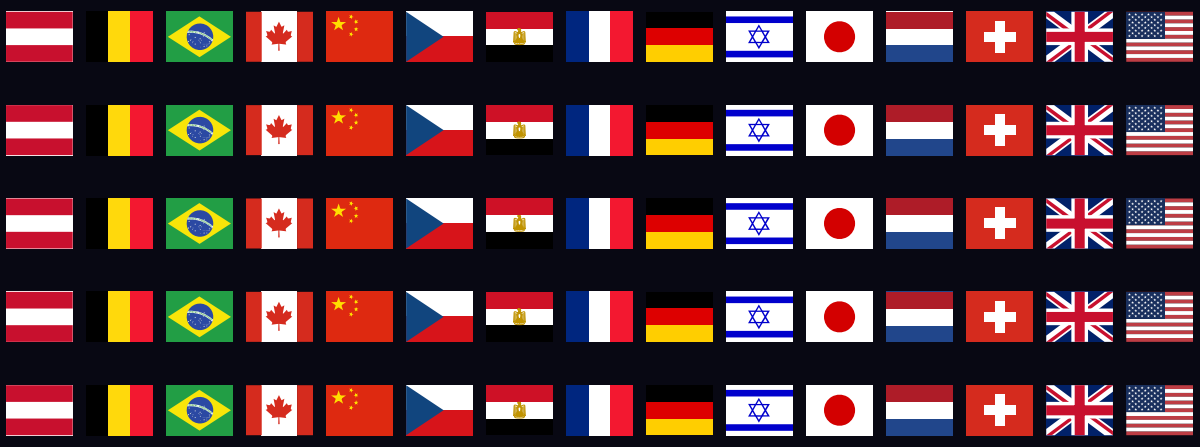
TECHNOLOGY M&A

Canada



LEXOLOGY
Getting The Deal Through

Consulting editor
White & Case

Technology M&A

Consulting editors

Arlene Arin Hahn, Neeta Sahadev

White & Case

Quick reference guide enabling side-by-side comparison of local insights into key laws, regulations and government approvals primarily implicated in technology M&A transactions; due diligence, including the transfer of licensed intellectual property, software due diligence, and the use of code scans; representations, warranties and other deal terms common to technology M&A transactions; and recent trends.

Generated 17 February 2023

Table of contents

Contributors

Canada

Michel Gélinas
mgelinas@dwpv.com
Davies Ward Phillips & Vineberg LLP

Gillian R Stacey
gstacey@dwpv.com
Davies Ward Phillips & Vineberg LLP

Elliot A Greenstone
egreenstone@dwpv.com
Davies Ward Phillips & Vineberg LLP

Tania Djerrahian
tdjerrahian@dwpv.com
Davies Ward Phillips & Vineberg LLP

Alexander Max Jarvie
mjarvie@dwpv.com
Davies Ward Phillips & Vineberg LLP

STRUCTURING AND LEGAL CONSIDERATIONS

Key laws and regulations

What are the key laws and regulations implicated in technology M&A transactions that may not be relevant to other types of M&A transactions? Are there particular government approvals required, and how are those addressed in the definitive documentation?

In Canada, jurisdiction is constitutionally divided between the federal government and the 10 provincial governments. There are also three territorial governments under the constitutional jurisdiction of the federal government, to which legislative authority can be delegated by the latter. The federal government has exclusive jurisdiction over some matters, whereas others are reserved to the provincial governments, and there are circumstances in which both levels of jurisdiction may apply to different aspects of the transaction.

Intellectual property (IP) is often an important aspect of technology M&A. In Canada, there are three primary IP statutes – all of which are federal – that can impact such transactions: the Patent Act , the Trademarks Act and the Copyright Act .

There is no Canadian statute that regulates trade secrets. Trade secrets can be protected contractually by common law in all provinces except Quebec, where matters relating to contracts, including the protection of trade secrets, are regulated by the Civil Code of Quebec .

There are federal and provincial statutes that govern the collection, processing, use and disclosure of personal information in ways that are more likely to impact technology M&A transactions than other types of transactions. The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to the collection, use and disclosure of personal information in the course of any commercial activity within Canada, except where provincial legislation deemed substantially similar to PIPEDA applies.

Quebec, Alberta and British Columbia have each enacted legislation that is substantially similar to PIPEDA. The provincial legislation generally applies to the intra-provincial collection, use and disclosure of personal information for private sector businesses in the relevant province (except Quebec, which claims jurisdiction over federally regulated businesses operating in the province). PIPEDA applies to transborder (whether provincial or international) data transfers. Amendments to Quebec's provincial legislation coming into force in September 2023 will create new obligations in relation to transfers from Quebec.

Depending on the parties or the technology involved, other specific federal and provincial laws and guidelines may apply, including the following.

Competition Act

The Competition Act provides for a merger review regime. While some mergers are notifiable, all mergers can be the subject of substantive review.

ICA

The Investment Canada Act (ICA) governs the review of foreign investments by non-Canadians in Canadian businesses. ICA review can include a net benefit review and a national security review (the NSR Process).

The net benefit review process requires pre-closing approval by the government for acquisitions of control of Canadian businesses by non-Canadians that meet certain thresholds. The NSR Process may be invoked in respect of any acquisition of, or investment in, a Canadian business by a non-Canadian, and any establishment of a new Canadian

business by a non-Canadian.

This process can result in, among other things, a prohibition on completing an investment, a requirement to divest the investment or the imposition of other conditions.

Although the concept of national security is not defined in the ICA, government guidelines list factors that may be taken into account when assessing whether an NSR Process is likely to be triggered (eg, whether the investment is likely to enable espionage or affect national defence capabilities, critical infrastructure or delivery of critical goods and services to Canadians) – all of which are more likely to involve technology companies.

Proposed legislation to update and reinforce the NSR Process under the ICA provides that certain sectors (as yet undefined) will be subject to a new pre-closing filing and suspensory obligation under the ICA. Although the regulations have yet to define the sensitive sectors to which the new filing obligation would apply, they are likely to include businesses handling personally identifiable information of Canadians and certain sensitive technologies.

CASL

Canada's anti-spam legislation (CASL) applies to all private sector businesses and imposes restrictions on sending commercial electronic messages, installing computer programs, using electronic address harvesting tools, using misleading sender and subject matter information and altering transmission data in an electronic message. CASL purports to have extraterritorial reach for foreign companies conducting business in Canada.

Industry-specific regulations

Industry-specific regulations may also apply, such as in critical infrastructure, healthcare, plant breeders, integrated circuit topography, industrial design, fintech and dealings with public sector clients.

Law stated - 31 December 2022

Government rights

Are there government march-in or step-in rights with respect to certain categories of technologies?

There is no federal or provincial legislation providing the government with march-in rights with respect to inventions conceived or first actually reduced to practice either under contracts with a government or where a government has funded research and development; instead, the federal or provincial government funding, grant or contribution agreements will specify what rights the government may have. Such rights are not typically march-in or step-in rights, but rather requirements:

- to use the inventions for the benefit of Canadians; and
- not to dispose of inventions that a government has funded without the consent of the relevant government.

Recourse for failure to comply can include requiring repayment of government funds. In addition to the government, other funding providers such as the National Research Council Canada, the Canada Media Fund, the Société de développement des entreprises culturelles (in Quebec) and universities can impose various restrictions on ownership, transfer and licensing as well as other terms and conditions that may impact transactions. Funding agreements must be included in due diligence and analysed in the context of a particular transaction.

Law stated - 31 December 2022

Legal assets

How is legal title to each type of technology and intellectual property asset conveyed in your jurisdiction? What types of formalities are required to effect transfer?

General

In general, legal title to any technology or IP assets is conveyed by the effect of the law (eg, in mergers) or contractually by assignment between the original right holder and the subsequent assignee. Best practice is to execute, in writing, any transfer or grant of IP rights, in whole or in part, including licences and security interests, and record them with the Canadian Intellectual Property Office (CIPO) to ensure a legal presumption of valid title, and better opposability and enforcement against third parties.

Patents

The first applicant to file a patent application for an invention is entitled to obtain the patent. A patent application can only be filed by the first and true inventor, the inventor's representative or an assignee. Companies should secure clear written assignment from third-party inventors, or have assignment provisions in their employment agreements or contractor agreements regarding ownership of inventions, patents and patent applications. Assignment of rights in patents and patent applications must be recorded with CIPO and executed in writing by at least the transferor, and preferably be witnessed. Assignment of rights that have not been recorded with CIPO may be considered void against a subsequent transferee.

Copyrights

Copyright arises automatically upon the creation of any new, original work that is fixed on a tangible support. By law, the author is the owner of copyrights in such work, except if the work was created by an employee in the course of employment. In that case, the employer is considered the first owner of copyright in the work.

Companies should secure clear written assignment from third-party authors or have assignment provisions in their employment or freelance agreements regarding ownership of copyrights in any work. To be valid, the assignment must be made in writing.

Although not mandatory, it is recommended that any assignment of rights in copyrights, in whole or in part, including licences and security interests, be recorded with CIPO to ensure presumption of valid title, and better opposability and enforcement against third parties. The Copyright Act also recognises certain moral rights of the author with respect to the work. These moral rights cannot be assigned but can be explicitly waived in writing, in whole or in part. The assignment of a copyright in a work does not, by that act alone, constitute a waiver of any moral right.

Trademarks

Legal rights to a trademark arise from the use of the mark in commerce or its registration. A trademark, whether registered or unregistered, is transferable, either with or separately from the goodwill of the business, for all or some of the goods or services for which it has been used or registered; however, assignment of trademarks without the associated goodwill may affect the distinctiveness of the mark and its subsequent validity or opposability.

It is therefore recommended that assignment of trademarks always include the goodwill of the business associated

therewith. Although not mandatory, it is recommended to have any assignment of rights in trademarks be made in writing, in whole or in part, including licences and security interests, and record them with CIPO to ensure presumption of valid title, and better opposability and enforcement against third parties. A trademark assignment can be recorded at CIPO at any time by the current owner, with or without supporting evidence, or by a third party with evidence of the transfer.

Trade secrets

A transfer of trade secrets is effected by contract. By their very confidential nature, assignment of trade secrets are not recorded on any specific registry or publicly disclosed.

Domain names

Domain names are typically registered with accredited registrars or through registration services. Typically, domain name transfers involve terminating the existing registrant's contract with the registrar and creating a new contract between the new registrant and the registrar for the right to use the domain name being transferred. Parties may enter into agreements to memorialise the conditions of the domain name transfer.

Law stated - 31 December 2022

DUE DILIGENCE

Typical areas

What are the typical areas of due diligence undertaken in your jurisdiction with respect to technology and intellectual property assets in technology M&A transactions? How is due diligence different for mergers or share acquisitions as compared to carveouts or asset purchases?

Typical areas of intellectual property (IP) and technology due diligence undertaken in Canada with respect to technology M&A transactions include identifying, reviewing and analysing, as appropriate, all:

- registrations and applications for IP assets owned by the target and confirming the status, lien status, chain-of-title, expiration date (if applicable), scope of protection and ownership thereof;
- unregistered IP assets owned or used by the target and confirming the ownership thereof, any restrictions thereon and the target's scope of rights therein;
- agreements with past and present employees and contractors with respect to the creation and ownership of IP assets, the assignment of IP rights and waiver of any moral rights therein and the protection of trade secrets and other confidential information;
- inbound and outbound grants or licences of IP rights granted by or to the target, and all other IP-related agreements (or IP provisions in agreements);
- target's processes for IP clearance, protection and enforcement, and for protecting trade secrets and confidential information;
- agreements for funding (whether from public bodies or private entities) of IP creation, co-development and joint ownership;
- past, present or threatened IP-related claims or disputes involving the target;
- processes and procedures for developing software code, including identifying open source or copyleft code, reviewing source code scans and identifying third-party access to the code;

- agreements and rights with respect to information technology (IT) assets and equipment;
- physical, technological and organisational IT security measures to assess potential security flaws, alignment with industry standards and the protection of personal information;
- practices with regard to the collection and processing of personal information to understand exposure to or compliance with privacy and data security laws and Canada's anti-spam legislation (CASL), contractual obligations and company policies; and
- data privacy breaches or security incidents and determining whether and what rights to use personal data will transfer to the buyer.

Although the due diligence process for mergers, share acquisitions, carve-outs and asset purchases are similar, there are several key differences. Because carve-outs and asset purchase transactions require the assignment and transfer of IP rights from the seller to the buyer, the buyer should confirm that all desired IP assets can be transferred (and are properly transferred) under applicable law.

If source code or data is being transferred, the right of the seller to transfer any third-party code (including open source) or third-party data (including personally identifiable information) should be properly vetted. The buyer should confirm that its intended uses of the data are permissible.

The buyer should review material IP and IT contracts to determine whether they include change of control provisions or anti-assignment provisions triggered by the contemplated transaction.

If a carve-out or asset purchase transaction does not include all employees or IP assets relevant to the purchased business, the buyer should perform sufficient diligence to confirm:

- that there is no 'key individual' risk;
- whether the seller will need to give or receive any transition services;
- whether any IT systems or data will need to be migrated or separated; and
- whether the buyer will be able to use, maintain and exploit the purchased IP assets post-closing.

Law stated - 31 December 2022

Customary searches

What types of public searches are customarily performed when conducting technology M&A due diligence? What other types of publicly available information can be collected or reviewed in the conduct of technology M&A due diligence?

- Searches of public court dockets to determine whether the target has been involved in litigation;
- searches of websites owned by the target to analyse privacy policies, terms of service and other publicly available information regarding the target;
- lien and security interest searches in each relevant province;
- security searches under section 427 of the Bank Act;
- bankruptcy searches;
- corporate registry searches; and
- off-title searches with various tax agencies, tribunals, commissions and government bodies.

Law stated - 31 December 2022

Registrable intellectual property

What types of intellectual property are registrable, what types of intellectual property are not, and what due diligence is typically undertaken with respect to each?

In Canada:

- patents are registrable with the Canadian Intellectual Property Office (CIPO), and issuance of a patent is required for patent protection;
- copyrights are registrable with CIPO, but registration of copyright is not required;
- trademarks are registrable with CIPO, but registration of a trademark is not required;
- trade secrets are not registrable;
- domain names are registrable with a certified domain name registrar, and registration is required; and
- industrial designs are registrable with CIPO, and registration is required.

The buyer should conduct the following searches on registrable intellectual property (IP):

- CIPO for registration of IP rights and its assignment;
- lien searches for grants of security on the registered IP; and
- searches of public court dockets to determine whether the seller has been involved in any IP-related litigation or any litigation related to its IP assets.

Law stated - 31 December 2022

Liens

Can liens or security interests be granted on intellectual property or technology assets, and if so, how do acquirers conduct due diligence on them?

Liens and security interests can be granted on IP and technology assets in Canada. The federal government has legislative authority over IP, but personal property security is primarily under provincial jurisdiction. Unless the borrower's operations are localised in one province, the lender may have to effect registrations in a number of jurisdictions across Canada to protect its security interest.

Ontario's Personal Property Security Act (PPSA) is modelled on article 9 of the US Uniform Commercial Code. All other Canadian common law provinces have similar PPSA-type legislation. The Civil Code of Quebec provides for a single form of consensual security: the hypothec (mortgage).

The federal IP statutes do not deal comprehensively with the taking of security interests in IP; however, security agreements can generally be filed against IP that is registered with CIPO. If a debtor's IP is of significant value, a lender will generally register security both provincially and federally.

Searches in the PPSA registry against the debtor name, and any predecessor names, in the relevant Canadian common law provinces (and the equivalent in Quebec) must be undertaken to determine if the target has granted security interests in its personal property that would include IP or technology assets. Unregistered security interests may also exist but will not have priority over registered security interests. Searches in the CIPO registry will disclose any IP registered in the name of the debtor as well as any assignments, licences or security agreements that have been registered against such IP.

Law stated - 31 December 2022

Employee IP due diligence

What due diligence is typically undertaken with respect to employee-created and contractor-created intellectual property and technology?

From an IP and technology perspective, the due diligence would focus on the following (redacted as necessary to comply with applicable privacy laws):

- all employment contracts, executive employment agreements, confidentiality and non-competition agreements entered into by the target with any of their officers or employees;
- all management, consulting and service agreements or other arrangements entered into by the target with respect to individuals who provide services to the target such as independent contractors and freelancers;
- copies of all agreements with employees, consultants and independent contractors relating to ownership and assignment of IP rights;
- copies of employment policies and handbooks, including those relating to invention disclosure and assignment and to the use or incorporation of open source and other third-party program code; and
- confirmation that all foreign workers (permanent and temporary), which could include, for example, a foreign PhD student enrolled at a Canadian university, have valid work permits.

Law stated - 31 December 2022

Transferring licensed intellectual property

Are there any requirements to enable the transfer or assignment of licensed intellectual property and technology? Are exclusive and non-exclusive licences treated differently?

In general, licences will specify the parties' rights and obligations in respect of assignment. Exclusive and non-exclusive are not treated differently. Without an assignment clause, the parties must consider the rules under the governing law of the licence.

In the common law provinces, if there is no assignment clause in the licence, the legal right or benefit arising under a contract can be assigned without the consent of the other party to the contract while the obligations or duties under a contract cannot be transferred without the consent of the other party. This does not mean, however, that the other party will be entitled to refuse to accept performance of obligations under the contract by a party other than the original party to the contract. Often, if one party to a contract assigns its rights to a third party, it will require the assignee to perform its obligations under the contract on its behalf and, in general, a delegation of contractual obligations is not a breach of the licence.

In Quebec, assignment is thought of as a single juridical act, and consent is necessary for the assignment of a contract to be valid. Consent can be given in advance through an assignment clause or afterwards through conduct.

Law stated - 31 December 2022

Software due diligence

What types of software due diligence is typically undertaken in your jurisdiction? Do targets customarily provide code scans for third-party or open source code?

In addition to technical due diligence on the software and IT systems of the target done by IT personnel or external consultants, legal due diligence on the following information will be undertaken:

- list of any software owned by the target and copies of all agreements related thereto;
- list of any third-party software used by the target, identifying those that are material, and copies of all agreements related to software;
- all other agreements with third parties relating to the target's use of software;
- a copy of all policies and procedures of the target relating to compliance with the terms of software licences, data security, open source code, cybersecurity and business continuity;
- details regarding any upcoming software or IT systems upgrades;
- details regarding issues with software (including service interruptions and cyber or data security breaches); and
- details regarding vulnerability scans and penetration tests undertaken by the target.

Targets will often provide open source code audits that identify the licence type for each library or other open source code element in use.

The extent of the software due diligence will depend on the importance of the software to the target and whether the target will be merged into the buyer's IT set-up post-closing.

Law stated - 31 December 2022

Other due diligence

What are the additional areas of due diligence undertaken or unique legal considerations in your jurisdiction with respect to special or emerging technologies?

AI

Canada has pending draft legislation that would regulate international and interprovincial trade and commerce in artificial intelligence (AI) systems by requiring that certain persons adopt measures to mitigate risks of harm and biased output related to high-impact AI systems. This legislation would be one of the first to regulate a specific software technology in common use. If enacted, it could have far-reaching implications for technology transactions, for every aspect from undertaking due diligence of the AI technology itself and the disclosure compliance by the target, through to post-close compliance and risk assessment.

IoT

In addition to IP due diligence, some internet of things (IoT) risks that are generally assessed include:

- the IoT-connected devices' security, encryption and privacy controls;
- the lifespan of the devices and their software update schedules;
- their potential as entry points for malicious actors into other computer networks and systems;
- their potential for government, law enforcement and commercial monitoring of consumers' and businesses' daily activities;
- their potential for cross-device tracking;
- their risk of threat to public safety; and
- their usage of algorithms that can lead to discriminatory decisions.

There is no specific law governing IoT, but the Office of the Privacy Commissioner of Canada published in 2020 guidance to IoT manufacturers on their responsibilities to protect personal data in line with the Personal Information Protection and Electronic Documents Act.

Autonomous driving

Autonomous driving is regulated provincially. Currently, fully autonomous vehicles are not permitted on public roadways. There is a legal framework governing the development, testing and deployment of autonomous driving as part of several provincial pilot programmes. The legal framework for the operation of autonomous vehicles has yet to be developed.

Diligence relating to adherence to applicable pilot programme requirements and customary considerations relating to IP rights in the technology, security and privacy, and product liability applies.

Big data

The Competition Bureau has publicly stated that it will consider the implications of big data (including collection, use and access to such data) in the context of a merger review, abuse of dominance cases, cartels and the application of the misleading representations provisions of the Competition Act. In the M&A context, this could impact:

- companies using algorithms to monitor competitors' pricing or make dynamic pricing decisions; and
- the evaluation of mergers where one of the parties has significant data, by taking into account the effects of the proposed transaction on non-price effects such as privacy, quality and innovation.

Law stated - 31 December 2022

PURCHASE AGREEMENT

Representations and warranties

In technology M&A transactions, is it customary to include representations and warranties for intellectual property, technology, cybersecurity or data privacy?

Technology M&A transactions will, depending on the type of technology involved, include representations and warranties (R&Ws) for intellectual property (IP), technology, data privacy and cybersecurity. The details and scope of these R&Ws depend on the circumstances, including whether the deal is structured as a share or an asset deal, the type of technology, the strategic reason for the acquisition, whether the IP pertains to an established business or a start-up, the bargaining power of the parties and how the parties wish to allocate risk.

These R&Ws may overlap with more general R&Ws and with each other. Additionally, when such R&Ws pertain to matters of significance to the acquisition, they may be subject to a separate indemnification regime or even be treated as fundamental R&Ws, which results in such R&Ws not being subject to time or other indemnification limitations that would otherwise generally be applicable.

IP

The types of IP R&Ws that are included depend on the nature of the target's technology and the value of its IP assets. IP R&Ws will typically address the following matters:

- a list or description of all IP owned by the target, whether such IP is registered or subject to an application and details in respect thereof;
- a list of all inbound and outbound licences and IP agreements to which the target is a party (including whether the target is licensing the IP in or out) and copies or descriptions of such agreements;
- whether the IP agreements to which the target is the party are in full force and effect and whether any party is in breach of or default under, or has provided or received any notice of breach of, default under or intention to terminate such agreement;
- whether there are any encumbrances on the IP owned by the target;
- whether the target's ability to sell, transfer, assign or convey IP is limited or whether it has granted any option to acquire any rights to or licences to use any of the IP;
- whether the target has a valid licence to use the IP it does not own;
- whether there are claims in progress, pending or threatened against the target relating to IP that it owns or licenses;
- whether the conduct of the target violates IP rights held by others;
- whether any person has infringed upon, violated or misappropriated the IP or otherwise used any of the IP in a manner that interferes with the target's rights to the IP;
- whether the target uses or makes available user-generated content; and
- for owned IP, whether it (1) was developed exclusively by the employees, contractors or subcontracted persons in the course of their employment or engagement, as the case may be, with the target; and (2) contains any IP owned or developed by any other person that the target has not acquired the necessary rights for its use.

Technology

From a technology perspective, purchase agreements will often include R&Ws on information systems, such as whether:

- the target business owns or has a valid right to access and use all software, hardware, telecommunications, network connections, peripherals and related communication and technology infrastructure that it uses;
- the target's information systems adequately meet the data processing and other information technology (IT) needs of the target;
- the target has all necessary software licences required to conduct its business;
- the target has measures in place to safeguard the information systems and whether such measures are respected and maintained in a manner consistent with industry standards and practice;
- the IT equipment and related systems owned or used by the target have been the subject of a security breach, material failure, breakdown, performance reduction or other adverse event that has caused or would reasonably be expected to cause any substantial disruption to their use, the target's business or any of its personnel, property or other assets; and
- the target maintains backup systems and disaster recovery and business continuity plans to ensure the continuing availability of the functionality provided by the information systems in the event of any malfunction of, or other form of disaster (including, without limitation, ransomware) affecting, the information systems.

Data privacy and cybersecurity

With the heightened focus of legislatures on data privacy, it has become standard to ask for and receive privacy R&Ws.

The scope and length of privacy R&Ws will depend on how much the target's business involves the collection and use of personal information, as well as the privacy laws that are applicable to the target. Making these determinations

depends on various factors, including the type of personal information, whose information it is, the nature of the target's business and whether such information crosses provincial borders and national borders. Consumer-facing businesses and service providers that process personal information on behalf of other businesses are generally regarded as having a higher-risk profile relative to other businesses.

Privacy R&Ws can address a number of matters, including:

- the target's privacy policies regarding the collection, use and disclosure of personal information (such as whether one is in place and whether it is being complied with in the course of operations by the business);
- the applicable privacy and data protection laws and whether the target is and has been in compliance with such laws;
- whether the target has received enquiries from or been subject of or to any complaint, audit or legal proceeding by any individual or government authority regarding personal information;
- whether the target is in compliance with privacy and data security obligations in respect of contracts to which it is party;
- whether the target has put appropriate contractual protections in place with its service providers that process or access personal information under the target's custody or control; and
- whether the target has experienced any loss, damage, unauthorised access, disclosure or use of any personal information in its possession, custody or control, or otherwise held or processed on its behalf.

Businesses with significant international flows of personal information will have higher burdens with respect to R&Ws relating to compliance with all applicable privacy and data protection laws. That said, because the Personal Information Protection and Electronic Documents Act has been deemed adequate by the European Commission relative to the European Union's General Data Protection Regulation (GDPR), the compliance burden with respect to personal information flows from the European Union to Canada is lessened in certain respects (eg, the circumstances in which GDPR-compliant standard contractual clauses are required will be limited).

Privacy R&Ws are closely connected to cybersecurity R&Ws as personal information is largely stored, processed and communicated electronically. The growing number of significant data breaches in recent years has also highlighted the financial and reputational risk associated with a breach.

Cybersecurity is often addressed as part of the privacy or the technology R&Ws, although it is now sometimes addressed as a separate heading. Cybersecurity R&Ws can address a number of matters, including:

- whether the target has been the subject of a data or security breach; and
- whether the target's cybersecurity practices comply with customary practice.

The governance, security and ethical handling of personal information may also, depending on the growth phase and the context of the target business and the nature of the purchaser, be a factor in environmental, social and governance assessments.

Law stated - 31 December 2022

Customary ancillary agreements

What types of ancillary agreements are customary in a carveout or asset sale?

In the context of a technology M&A transaction, a carve-out can require a number of ancillary agreements related to intellectual property (IP), depending on whether the IP is used solely by the carve-out business or both by the seller and

the carve-out business, and on who owns the IP. If the seller owns the IP needed by the carve-out business but also needs it to operate the business it retains, a licence between the seller and the buyer will be required; otherwise the seller can sell the IP to the buyer. If the seller licenses the IP needed by the carve-out business from a third party, either consent will be required or a new licence may be needed.

Further, depending on the independence of the carve-out business from the rest of the seller's operations and the buyer's ability to immediately assist the carve-out business, a transition services agreement may be needed for some period post-closing to deal with essential services that have up to the date of closing been provided to the carve-out business by the seller. Services covered can include a number of matters, including IT matters.

Even in non-carve-out transactions, asset deals will have particular ancillary agreements that a share deal will not. Of note is the employment context. In the common law provinces of Canada, individual employment contracts or offer letters will be required from the buyer as employees are presumed to be terminated with an asset deal. This does not apply in the province of Quebec where the contracts of employment are not terminated by the alienation of the business and are binding on the purchaser. Agreements dealing with other terms of employment such as long-term incentive compensation, may also be implemented, especially if employees can no longer participate in the long-term incentive plans of the seller (stock option plans, etc).

Additionally, like in any other M&A transaction, non-competition agreements can be desired. In Ontario, legislation generally prohibits employers from entering into non-compete provisions; however, the use of non-competes in the context of a business acquisition and for a defined class of executives remains permitted.

Law stated - 31 December 2022

Conditions and covenants

What kinds of intellectual property or tech-related pre- or post-closing conditions or covenants do acquirers typically require?

Interim period covenants

As with any M&A deal, technology deals will typically include the following covenants from the seller to:

- notify the buyer of any breach of representation, warranty or covenants, including those related to IP and information technology (IT);
- conduct the business in the ordinary course;
- preserve the goodwill of the target business;
- comply with applicable laws; and
- notify, or get approval from, the buyer of any actions, notices and communications by government bodies.

Additionally, depending on the technology and what was identified during the due diligence process, specific IP, technology, privacy and cybersecurity covenants may be found, such as:

- a restriction on the sale, assignment or transfer of some of or all the IP or technology assets;
- a restriction on the granting of security on some of or all the IP or technology assets;
- an obligation to maintain ownership, validity and enforceability of some of or all the target's IP registrations;
- an obligation to protect the confidentiality and value of trade secrets and other IP;
- making filings to ensure that (1) the chain of title of each IP registration reflects all prior acquisitions and transfers and the release of any prior security interests, and (2) that the seller is the current owner of record, without a break in the chain of title;

- registering new IP or filing new applications; and
- requiring the target to remediate known privacy and cybersecurity issues such as obtaining necessary consents or addressing security vulnerabilities.

Closing conditions

As with any M&A deal, technology deals will typically include the following conditions:

- accuracy of representations and warranties and compliance with covenants as reflected in a bring-down certificate;
- obtaining consents for any material contracts or permits needed for the target business;
- absence of any legal action or proceeding that would prohibit or otherwise impose material limitations on the buyer's ownership of the business or assets;
- absence of material adverse change with respect to the business or assets;
- receipt of the government approvals required to implement the transaction; and
- the signing of various agreements, such as non-compete agreements, employment agreements and transition services agreements.

Additionally, depending on the technology, the type of transaction and what was discovered during the due diligence process, specific IP, technology, privacy and cybersecurity covenants may be needed, such as:

- licences or transition services agreements between the buyer and the seller for retained or shared IP;
- consulting agreements where key employees with IP or IT knowledge are being retained by the seller but are needed by the buyer;
- milestones payments based on product launch or other metrics;
- IP assignment agreement or IP ownership confirmation from key employees and other parties; and
- covenants regarding founder support when the business relies on a user community.

Post-closing covenants

Depending on the technology, the type of transaction and what was discovered during the due diligence process, specific IP, technology, privacy and cybersecurity covenants may be found, such as:

- continued confidentiality in respect of the target business;
- obtention of consents in terms of any material contracts or permits not obtained prior to closing;
- provision of notice of the transfer of personal information and obtention of new consents regarding information and data protected by privacy legislation (eg, new uses of the data); and
- collaboration in terms of post-closing registrations.

Law stated - 31 December 2022

Survival period

Are intellectual property representations and warranties typically subject to longer survival periods than other representations and warranties?

In deals without representations and warranties (R&Ws) insurance, the survival period for most R&Ws is 12 to 24 months. Where R&Ws for IP pertain to matters of significance to the acquisition, they can be designated as fundamental or be subject to a specific regime, carving them out of the general survival period and making them longer. Sometimes, in the software and video game industries, the survival period can be tied to product launch, but the parties normally provide for a drop-dead date if there is an unforeseen delay in the product launch.

In deals with buy-side R&Ws insurance, survival periods can be shortened as coverage is provided by the policy, which will typically provide for three years of coverage for non-fundamental R&Ws and six years for fundamental R&Ws regardless of survival periods under the purchase agreement. Increasingly, there are 'no-survival' deals with R&Ws insurance where the seller's R&Ws do not survive the closing and the buyer has to rely on the R&Ws insurance in the case of R&Ws breaches.

Law stated - 31 December 2022

Breach of representations and warranties

Are liabilities for breach of intellectual property representations and warranties typically subject to a cap that is higher than the liability cap for breach of other representations and warranties?

Liabilities for breach of IP R&Ws may be subject to a cap that is higher than the liability cap for breach of other R&Ws in certain cases, such as where they are considered fundamental to deal.

Law stated - 31 December 2022

Are liabilities for breach of intellectual property representations subject to, or carved out from, de minimis thresholds, baskets, or deductibles or other limitations on recovery?

As with other R&Ws, liabilities for breach of IP R&Ws are normally subject to baskets and caps, unless specifically carved out, for example, as a result of being a fundamental representation and warranty.

In deals with R&Ws insurance, certain IP and technology issues may be excluded and therefore need to be addressed by a stand-alone indemnity.

Law stated - 31 December 2022

Indemnities

Does the definitive agreement customarily include specific indemnities related to intellectual property, data security or privacy matters?

Specific or stand-alone indemnities are typically used as a way of addressing risks for which the buyer does not wish to assume responsibilities (or, if applicable, are excluded from the R&Ws insurance policy) and are often related to issues identified during the buyer's due diligence and not otherwise dealt with by a renegotiation of the purchase price. In the M&A technology sphere, examples include:

- known litigation such as those dealing with IP infringement, privacy or cybersecurity claims made by or against the target;
- known breaches of law or licence agreements; and
- known product liability issues.

In an asset purchase agreement, a typical stand-alone indemnity is one that covers liabilities retained by the seller.

Law stated - 31 December 2022

Walk rights

As a closing condition, are intellectual property representations and warranties required to be true in all respects, in all material respects, or except as would not cause a material adverse effect?

IP R&Ws form part of closing conditions through their bring-down at closing.

Where the IP R&Ws are not of great significance, the bring-down of such R&Ws will be subject to a materiality standard; however, if those IP R&Ws are themselves already qualified by a materiality standard, the buyer will not want a double materiality standard and will ask that such R&Ws be, upon their bring-down at closing, 'true and correct in all respects' rather than 'true and correct in all material respects'.

Where the IP R&Ws are of great significance and the buyer has bargaining power, the IP R&Ws can be treated as 'fundamental' R&Ws requiring them to be 'true and correct in all respects' upon bring-down at closing.

Law stated - 31 December 2022

UPDATES AND TRENDS

Key developments of the past year

What were the key cases, decisions, judgments and policy and legislative developments of the past year?

Legislative developments

There are a variety of legislative developments – whether recently enacted, under consideration by legislatures or published as white paper proposals – that could have a significant effect on technology transactions. These span a wide range of issues, including:

- changes to the private sector privacy laws, including new fines and penalties, and expanded powers for privacy regulators;
- new draft legislation governing the development and use of artificial intelligence technologies;
- new telecommunications regulator powers over online streaming services and digital news intermediaries;
- new laws governing cybersecurity;
- extensions to the term of copyright protection;
- new legislation governing personal health information; and
- new requirements relating to the use of the French language in Quebec.

More specific legislation related to the above includes the following:

- Federal Bill C-27, the Digital Charter Implementation Act 2022, tabled by the federal government on 16 June 2022;
- Federal Bill C-19, the Budget Implementation Act 2022, No. 1, which received royal assent on 23 June 2022 and will make amendments to the Copyright Act;

- Federal Bill C-11, the Online Streaming Act, introduced on 2 February 2022;
- Federal Bill C-26, an Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, introduced on 14 June 2022;
- Federal Bill C-18, the Online News Act, introduced on 5 April 2022;
- Quebec Bill 64, an Act to modernize legislative provisions as regards the protection of personal information, which received royal assent on 22 September 2021;
- Quebec Bill 6, an Act to enact the Act respecting the Ministère de la Cybersécurité et du Numérique and to amend other provisions, which received royal assent on 3 December 2021;
- Quebec Bill 96, an Act respecting French, the official and common language of Quebec, which received royal assent on 1 June 2022;
- Quebec Bill 3, an Act respecting health and social services information and amending various legislative provisions, introduced on 7 December 2022; and
- Government of Ontario White Paper, Modernizing Privacy in Ontario, released on 17 June 2021, outlining a proposed Ontario private sector privacy law.

Key cases, decisions and judgments

On 25 November 2022, the Court of Appeal of Ontario in Owsianik v Equifax Canada Co , 2022 ONCA 813, decided that the tort of inclusion upon reclusion cannot be a cause of action against defendants whose negligence in storing information led to a privacy breach.

On 27 May 2022, the Federal Court in Rogers Media Inc v John Doe 1 , 2022 FC 775, issued a dynamic site-blocking order to force internet services providers to block unlawful streaming of live broadcasts of National Hockey League matches in Canada whose copyrights are owned by the plaintiffs.

The authors would like to thank Hélène Bussières for her assistance in the preparation of this chapter.

Law stated - 31 December 2022

Jurisdictions

Austria	Schoenherr
Belgium	Agio Legal
Brazil	Azevedo Sette Advogados
Canada	Davies Ward Phillips & Vineberg LLP
China	White & Case
Czech Republic	White & Case
Egypt	Zaki Hashem & Partners
France	White & Case
Germany	White & Case
Israel	Erdinast, Ben Nathan, Toledano & Co
Japan	Nagashima Ohno & Tsunematsu
Netherlands	Van Doorne
Switzerland	Walder Wyss Ltd
United Kingdom	White & Case
USA	White & Case