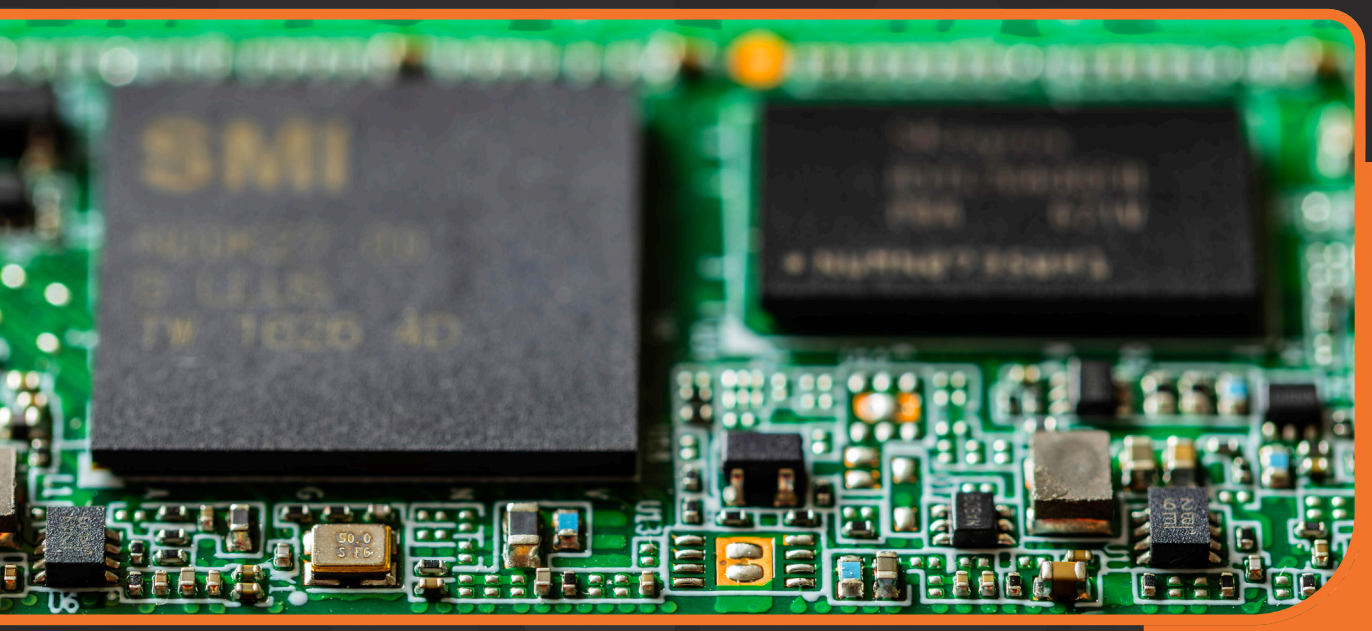
International
Comparative
Legal Guides



Practical cross-border insights into technology sourcing

Technology Sourcing 2023

Third Edition

Contributing Editor:
Mark Leach
Bird & Bird LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Canada


Robert Piasentin


Greg Johns


Yue Fei


Anika Klassen

McMillan LLP

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

Canadian procurement of technology products and services is not generally governed by legislation, but rather is informed by common law and administrative law, as parties typically navigate a binding request for proposal process. Certain technologies may however be subject to mandatory or discretionary procurement requirements (e.g., a business that deals with virtual currencies must adhere to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* ("PCMLTA") by establishing a compliance program, identifying and verifying clients, keeping adequate records, and reporting suspicious transactions).

In response to the proliferation of artificial intelligence ("AI") services and the potential corresponding use, disclosure and processing of data and personal information through AI, the Canadian government has introduced the *Artificial Intelligence and Data Act* ("AIDA") as a part of Bill C-27. AIDA, should it be passed into law, aims in part to regulate the design, development and use of AI systems to promote responsible adoption of AI technologies by Canadian businesses. The second reading of Bill C-27 by the House of Commons occurred on 24th April 2023 and has since been referred to committee for consideration. Currently, AIDA does not specifically target private sector procurement directly; however, its scope captures technology in the private sector, which means that Canadian businesses need to be diligent to understand the impact AIDA could have on their operations.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Public sector procurement of technology products and services will generally be subject to obligations originating from: (i) public sector privacy legislation, if the technology products and services involve the collection, use, retention or disclosure of personal information; (ii) applicable trade laws, which include signed international trade agreements and the domestic Canadian Free Trade Agreement ("CFTA"), whose primary objective is to "reduce and eliminate, to the extent possible, barriers to the free movement of persons, goods, services, and investments within Canada and to establish an open, efficient, and stable domestic market"; and (iii) certain international trade treaties or agreements to which Canada is a party.

Public Services and Procurement Canada, the Canadian federal procurement and purchasing office, also publishes a Code of Conduct for procurement, along with policies and directives to guide the framework for federal purchase of goods and services, in addition to providing a challenge process for procurement conduct claims.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No, Canadian law does not impose any minimum or maximum term for such contracts.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No. However, in certain circumstances equitable principles may apply to require a reasonable notice period for termination (for example, if the relationship involves a significant imbalance of power, if a customer's business accounts for a significant source of a supplier's income, or if one party is otherwise highly dependent on the other party).

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

In Canada, parties are required to act in good faith in the performance of contractual obligations. In *Bhasin v. Hrynew,* 2014 SCC 71, the Supreme Court of Canada ruled that there is a general organising principle of good faith in the law of contract, and that parties must perform their contractual duties honestly and reasonably and not capriciously or arbitrarily. The Supreme Court of Canada further developed this concept in *Wastech Services Ltd. v. Greater Vancouver Sewerage and Drainage District,* 2021 SCC 7 by ruling that parties to an agreement need to exercise any discretion under a contract so as to be consistent with the actual purpose for which that discretion was granted.

Note that the Civil Code of Quebec (see Articles 6 and 7) establishes a duty of good faith which applies to any negotiations of agreements or their subsequent performance.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

A customer can recover damages in the event the supplier breaches its contract with the customer. If the supplier fails to perform its obligations under the contract, the customer may also seek injunctive relief, specific performance, and other equitable remedies.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

Remedies or protections for a customer in such contracts typically include: representations, warranties and covenants related to the technology solutions or services and the underlying intellectual property; supplier indemnities; issuance of service credits; holdbacks or reductions in fees; access to the supplier's intellectual property (in escrow); termination rights in the event of a breach by the supplier; inclusion of performance bond requirements, and transition assistance.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

A party may terminate a contract without giving rise to a claim for damages from the other party: (a) upon mutual agreement with the other party; (b) for convenience upon notice to the other party (subject to possible termination payment obligations associated with this method of termination); (c) upon notice for a breach of any contractual obligations by the other party (subject to a reasonable cure period); (d) upon the occurrence of a *force majeure* event; (e) if the contract is frustrated; (f) upon a change in control; or (g) upon bankruptcy or insolvency of the other party.

2.7 Can the parties exclude or agree additional termination rights?

Yes, the parties are generally free to exclude or agree to additional termination rights (subject to public policy). Some of the additional termination rights which may be included are termination for an uncured material breach or a recurring breach of the agreement or service levels.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Contracting parties are generally free to limit or exclude their liability under Canadian law. However, the limitation or exclusion may not be enforceable if it is interpreted to be unconscionable (e.g., inherently unfair) or against public policy (e.g., limit or exclude liability for criminality or fraud). The parties will also negotiate exclusions on liability for indirect, incidental, consequential and punitive damages. These limitations and exclusions can take a variety of forms and so are generally subject to significant negotiation meaning they are often among the last provisions to settle.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Parties are free to agree financial caps on their respective liabilities under a contract and may include different caps for different liabilities. The concept of super caps for higher risk liabilities has become commonplace, which sets a higher dollar cap for liabilities such as IP infringement and data breaches. The nature of the services being provided as well as the nature of the parties and their industry will all have an impact on the final agreed caps.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, these general principles would also apply to the technology procurement contracts mentioned above.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

The most common method of dispute resolution in technology contracts is the inclusion of a tiered dispute resolution clause. This method includes an escalating series of steps in the dispute resolution process, encouraging parties to resolve a dispute through alternative methods before engaging in arbitration or litigation.

In addition to this tiered process, technology contracts often include procedures that will help simplify the dispute resolution process by fixing certain procedures, including direction on what laws will apply, in which jurisdiction the dispute will be resolved, the process for selecting a mediator or arbitrator, and setting time limits for each step within the dispute process. Further, many technology contracts include "self-help" provisions that provide a party with certain written assurances if the other party fails to perform its obligation under the contract (e.g., holdbacks of payments if a deliverable or service is inadequate).

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

In Canada, IP rights are protected for the most part under statute in the first instance. Parties will then generally seek to protect their IP interests through specific steps including performing extensive due diligence, verifying ownership, and carefully negotiating IP-specific contractual obligations. The final outsourcing agreement will generally contain express provisions identifying who owns which works (pre-existing works versus works made under the agreement), the scope of any licences specific to that owned IP, and how such IP and related works can be used. A requirement to deposit key software into escrow can also be used as a tool for securing access to core technologies.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Assignments of intellectual property rights should be in writing. It is worth noting that a Canadian copyright holder cannot assign its moral rights; parting with moral rights requires an explicit waiver and such a waiver is important in any assignment. Assignments of patent rights, industrial design rights and copyrights should be recorded with the Canadian Intellectual Property Office ("CIPO"), to protect the assignee from a situation whereby a subsequent assignee's claim takes priority over an unregistered assignee's claim. For trademarks, although there is no requirement to record assignments of trademarks with CIPO, recording can simplify subsequent transfers and protect a transferee from competing third-party interests by notifying the public of the transfer. However, the assignment of an unregistered common law trademark cannot be recorded with CIPO.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Know-how, trade secrets and business confidential information are not governed through legislation but are rather protected under common law. Contracts will often specifically set out the protections to be granted to know-how, trade secrets and confidential information. In addition, a party can rely on the common law for an infringement of a trade secret by considering factors such as money and time invested in development, measures taken to preserve secrecy, and whether misuse harms the owner.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

On a national level, Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA") governs how federal works, businesses, or undertakings collect, process and disclose personal data in the course of commercial activity. PIPEDA also applies to private sector organisations that collect, use, and disclose personal data in provinces which do not have substantially similar legislation. Currently, Alberta, British Columbia and Quebec have legislation that is deemed substantially similar to PIPEDA and in those provinces, the provincial legislation will govern data protection activity which occurs entirely within that province's borders. Certain provinces also have legislation which applies specifically to the protection of privacy in health information which could also apply in a technology sourcing transaction.

Any technology sourcing agreement will address the treatment of personal data to ensure compliance with privacy legislation. In particular, rights and obligations around consent, collection, storage, use and processing of personal data should be explicitly agreed to avoid potential disputes.

On 16th June 2022, the Federal Government tabled Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, also known as the *Digital Charter Implementation Act*. If passed, Bill C-27 will materially change the legal landscape for privacy and data protection in Canada.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

In Canada, PIPEDA governs the transfer of personal data across borders in a commercial context. While PIPEDA (nor the substantially similar provincial legislation) does not prohibit the transfer of personal data across borders into other provinces or countries, it imposes certain responsibilities and obligations on the transferor.

Under PIPEDA, an organisation is responsible for personal data in its possession. Organisations are required to provide a comparable level of protection when the information is being processed by a third party, irrespective of their location. If the information is being processed in a different province or country by a third party, the initial organisation needs to protect the data against unauthorised use and disclosures. Privacy regulators also require organisations to advise individuals that their personal data will be transferred to another jurisdiction and may, as a result, be accessed by courts, law enforcement, or security authorities of such jurisdiction.

Some provincial public sector privacy legislation also imposes restrictions on the public entity and any suppliers working with that public entity on transferring personal data outside of the province.

5.3 Are there any legal and/or regulatory requirements concerning information security?

Information security requirements are imposed by a number of different legal and regulatory frameworks. In particular, PIPEDA contains provisions that impose data protection requirements in the course of commercial activity. This includes a requirement that organisations impose security safeguards appropriate to the sensitivity of the personal information collected.

Certain sectors in Canada are also subject to sector-specific statutes that impose requirements on information security. For example, the federal *Bank Act* regulates the use and disclosure of personal financial information by banks.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

As a general rule, when employees are transferred between companies, their employment with the transferor company is terminated and they are hired as a new employee of the transferee. However, this is not always the case, and the answer depends on a variety of factors.

If the outsourcing is structured as an asset purchase, the answer is dependent on union status and jurisdiction. Jurisdiction depends on the nature of the business, as many are subject to provincial labour and employment laws, but certain industries and activities of an inter-provincial nature, may be subject to federal labour and employment laws. For non-unionised employees, in most Canadian jurisdictions, they are not transferred by operation of law. However, unionised employees may be transferred by operation of law if the outsourcing is

considered a "sale of a business", and their employment is continued following the sale or transfer of all or part of the business, subject to the terms of their collective agreement.

If the outsourcing is structured as a share transfer, there is no change to the employer recognised by employment law.

6.2 What employee information should the parties provide to each other?

Parties will generally share basic employee information, such as the number of employees and any material terms of their employment, including benefits, termination and change of control. However, any employee personal information must only be shared with consent of the employee or otherwise as permitted under Canadian privacy legislation.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

Subject to the terms of their employment agreement, an employer in Canada can dismiss an employee for any reason, so long as that reason is not discriminatory, at any time in accordance with applicable employment standards legislation. This is not unusual in a non-unionised setting. However, most unionised employees may be protected from termination, barring misconduct, under their collective agreement. The exception to this is where the collective agreement may permit layoffs due to a changed business environment.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

For non-unionised employees, yes. There are no specific restrictions to harmonisation of the terms of employment, but it is expected that the transferee will make the harmonised terms clear. An employee may be able to quit or claim constructive dismissal if harmonisation results in a material change without the employee's consent. In a unionised setting, any changes to the terms of the collective agreement must have the agreement of the union.

6.5 Are there any pensions considerations?

Yes. Generally, pension plans are employer-specific in Canada and are regulated under the applicable legislation based on the province of registration of the plan. The applicable considerations will be driven by the nature of the benefits provided by the outsourcing company, the jurisdiction, and whether employees are unionised. For example, a collective agreement may incorporate a defined pension plan that the transferee must mirror during outsourcing. Other considerations include how accruals will be handled during a temporary outsourcing period, and if there is need for any dispositions or transfers of pension assets. The rules regarding portability and accrual of benefits and the administration of the plan depends on the applicable legislation and the type of pension plan.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

Privacy is a key consideration, particularly if personal information will be transferred outside of Canada. It is critical that the appropriate consents are obtained and employee personal information that is being processed outside Canada is adequately protected with a comparable level of protection. It is also important to consider if employees will remain in the same, or similar, roles in connection with offshore outsourcing.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

Canada does not currently have any laws or regulations applicable broadly across all sectors that regulate outsourcing transactions.

However, if the outsourcing transaction involves the collection, use, disclosure, or other processing of personal information, privacy legislation and outsourcing guidelines published by privacy regulators in Canada must be taken into account.

In the financial services sector, federally regulated financial institutions ("FRFIs") must abide by the guideline Outsourcing of Business Activities, Functions and Processes (referred to as "OSFI Guideline B-10") published by the Office of the Superintendent of Financial Institutions ("OSFI"). If the entity doing the outsourcing is in another regulated sector, for example, healthcare, energy or gambling/lotteries, the sector specific regulations should be reviewed for any requirements applicable to outsourcing.

On 23rd April 2023, OSFI released an update to OSFI Guideline B-10 now titled "Third Party Risk Management Guideline" which broadened the focus of the guidance. This new guideline will come into effect on 1st May 2024 and requires FRFIs to have a risk management programme that governs all third-party arrangements (including for SaaS and cloud computing). The new OSFI Guideline B-10 should lead to FRFIs updating their approach to third-party risk management processes to implement clear governance and accountability structures that cover all types of third-party arrangements and require appropriate contract terms, taking into account the risk and criticality of each arrangement.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

Outsourcing contracts are typically structured under a master services agreement ("MSA") with attached schedules directly between the customer and the supplier. The MSA will set out the transition and steady state services, fees and payment terms, service levels, assets, key personnel, liability provisions, and termination rights, among others. Oftentimes a statement of work is used to describe the outsourcing services under an enterprise-level MSA for different types of technology services. Global contract structures are largely driven by tax requirements and often use an MSA with local implementation agreements between local customer and provider affiliates to avoid cross-border withholding taxes and tax residency rules.

Outsourcing agreements can also be incorporated into a corporate reorganisation or restructuring, as part of a broader joint venture arrangement between two or more parties, or even as a key component of merger and acquisition deal.

The updated OSFI Guideline B-10 further provides a list of contractual provisions that FRFIs should include in outsourcing contracts which represent high-risk and critical third-party

agreements. Such provisions should also be considered for other non-critical third-party contracts.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

There is a broad range of approaches to service levels and service credits ranging from simply addressing a few critical service levels (e.g., availability, response time) to complex methodologies providing for many service levels across multiple categories.

Service credits are typically calculated using a methodology based on a percentage of the monthly fees payable under the agreement. Most agreements also provide an aggregate cap on the maximum service credits payable in any monthly expressed as a maximum percentage of the monthly fees.

Some service levels may be designated key performance indicators (sometimes referred to as service level objectives) which do not trigger service credits and are addressed through governance and escalation. Where service credits are provided, service providers prefer them to be a customer's sole remedy but customers often object and negotiate this provision out, given the potential for significant damages.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

There are a broad range of charging methods depending on the type of outsourcing services. Most methods are based on a form of unit pricing together with a baseline number of units set out in the contract. There may be fixed charges for certain types of services like initial transition of functions and responsibilities to the outsourcing provider. It is less common but there may be pricing mechanisms for gain sharing of benefits and other incentive arrangements.

Outsourcing contracts also sometimes provide an adjustment mechanism if the consumption of units of services varies significantly due to extraordinary events like divestiture of a major business unit.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

In many third-party contracts, an assignment may be effected by obtaining the consent of the third party to the assignment, or by delivering notice of any such assignment to the third party. To determine whether consent or notice may be required, the third-party contracts need to be carefully reviewed and the outsourcing agreement should allocate responsibility for obtaining such consent.

It may be prudent to enter into a simple assignment agreement to transfer third-party contracts to a service provider. Such an assignment agreement would typically allocate liability for events and claims arising before and after the assignment effective date and would clearly identify each party's responsibilities.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

There are no taxes in Canada which specifically apply to technology outsourcing services. However, the federal government imposes a multi-stage value-added tax (referred to as the "GST"), which applies to all domestic supplies of services in Canada.

In addition, certain provinces in Canada have harmonised their sales taxes with the GST, resulting in a combined sales tax (referred to as the "HST"). Generally, entities providing outsourcing services in the course of carrying on business in Canada must register for GST/HST and collect, remit and account for such GST/HST.

Quebec imposes a multi-stage, value added tax (the "QST"), which is substantially harmonised with the GST/HST, but is administered by the Quebec tax authorities and has its own registration and compliance regime.

In cases where a foreign entity provides outsourcing services in Canada and is not a permanent resident for Canadian tax purposes, there would be withholding tax imposed under Canadian law on payments to the foreign entity.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

A first key issue for a customer to consider is whether an on-premise software licensing solution is actually the most suitable or appropriate for its business model. Cloud-based or software-as-a-service ("SaaS") models may be more useful or beneficial when considering factors such as whether a business prefers a subscription model over an outright purchase, whether the software will require frequent updates, whether the business has storage limitations, whether reliance on third parties is perceived as a benefit or hindrance, among other considerations.

If a customer opts to proceed with an on-premise software solution, a key consideration will be the scope of the customer's use and access rights granted in relation to the software, which should be clearly set out in the licence agreement. In addition, consideration must be given to the duration of the licence term to ensure that the customer has the rights it needs for its required term. Additional scope considerations are whether the licence allows back-ups, disaster recovery, third-party support, maintenance or access, server and business mobility restrictions, and geographic limitations.

Another consideration is the allocation of risk within the licence agreement. Who is responsible for providing and installing updates, patches, upgrades and bug fixes, at whose cost, and for how long? Maintenance and support of the on-premise software solution both during the term and following its expiration needs to be carefully considered and agreed upon.

Due to rapid development and advancements in technology, the customer will need to ensure that the software and relevant hardware remain compatible. In addition, if the business grows, will the licence terms allow for additional licence seats through an enterprise-wide licence or will additional licences be required to be purchased and, if so, at what cost? Relatedly, the outsourcing contract will need to address responsibility over security concerns related to the on-premise solution.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

A key issue to consider for maintenance and support services is related to resolution time for fixing any reported problems with the software, especially when the software plays a key role in the customer's business. The contract should clearly set out

the process for the customer to raise a ticket for any required maintenance and support along with the times for the service provider to respond and resolve the ticket, any escalation steps, and customer remedies if the issue is not resolved within the specified period.

It is also important to address scheduled and emergency maintenance and support which results in the customer's system being down, in particular by identifying when scheduled maintenance will occur, how frequently, how long it can last, and how much notice is required to conduct scheduled or emergency maintenance, among other issues. Customers should also consider their rights with respect to upgrades and new versions of the software and whether such upgrades or new versions are included in the fee, whether purchasing upgrades is a condition of ongoing maintenance, and whether the customer can delay upgrades.

It is also important to consider what types of maintenance and support services are included. For example, will maintenance and support cover the implementation of new releases, updates or bug fixes? If changes are introduced by the service provider, the customer will want to understand whether it has the ability to test and approve any new releases, updates or bug fixes before they go live to ensure that the changes are compatible with the customer's systems, and whether the customer is permitted to run or maintain multiple versions of the software for backup purposes, and if older versions of the software will be supported.

Finally, the customer will want to verify how the fees for any maintenance and support will be charged (included in software fees, annual fees, renewal costs, etc.) so that it has a clear picture of all costs with respect to the outsourcing arrangement without falling victim to any hidden or unforeseen fees.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Software escrow arrangements are commonly used in the event that a software licensor is no longer able or willing to maintain the software and the licensee requires access to the software for its key business purposes. A software escrow agreement sets out each party's responsibilities with respect to the source code in escrow and the specific release conditions.

In the event of the licensor's insolvency, a software escrow agreement will generally be enforceable if clearly drafted; thus, a customer will want to ensure that certain conditions are met. First, a reputable third-party escrow agent should be appointed by the licensor and licensee to hold the escrowed software and the agreement among the three parties needs to be clear and enforceable. Next, the escrow agreement must spell out exactly what must be deposited (source code, object code, documentation, data, etc.) and how frequently those deposits must be updated. Then, the release conditions in the escrow agreement are of fundamental importance. Lack of clarity or uncertainty as to when the escrow materials can be released will create material issues for a customer. Finally, the terms of the escrow agreement need to spell out the licence terms that will govern the customer's use of the escrowed materials upon their release. In some cases, the licence will be broad and allow the customer to modify, adapt, compile and use the escrow materials in whatever way the customer deems necessary, but often the licence grant will be narrower. The specific terms need to be carefully reviewed and agreed.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

There are no laws or regulations in Canada that specifically regulate the procurement of cloud computing services. However, industry and/or sector specific laws, regulations, guidelines or guidance documents may affect certain aspects of a cloud computing transaction. For example, privacy regulators in Canada have issued guidance documents regarding cloud computing and Canadian privacy legislation also imposes certain responsibilities, including in relation to the location of personal information, on customers when procuring cloud computing services.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Cloud computing solutions have been increasingly adopted by organisations of all sizes in both the Canadian public and private sectors due to a number of factors, but primarily because they have provided good financial value for organisations. Cloud computing services are delivered primarily in the following models in Canada: SaaS; platform-as-a-service ("PaaS"); and infrastructure-as-a-service ("IaaS"), with new cloud services being introduced including function-as-a-service ("FaaS") and backend-as-a-service ("BaaS"). Businesses looking to adopt cloud computing services will need to consider how they want to implement the cloud services. They can do so by engaging a public cloud service provider, where a cloud provider owns and manages the servers for many businesses, or they can implement a private cloud whereby it has its own cloud infrastructure, or a combination of the two. Choosing the right implementation model will be based on the particular risks and issues facing an organisation as businesses are often looking to keep mission critical technologies on a private cloud to retain control.

9.3 What are the key legal issues to consider when procuring cloud computing services?

The key legal issues to consider when procuring cloud computing services are primarily: (a) privacy and data security considerations; (b) location and segregation of data; (c) information security considerations; (d) control over and access to data; (e) suppliers' use of subcontractors in providing cloud computing services; (f) service failures and business interruption; and (g) transition back in-house or to a replacement supplier upon termination of services.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

Currently, there are no national laws or regulations in Canada specific to the procurement or use of AI-based solutions or technologies. Rather, such technologies are subject to legislation, such as the privacy laws which govern the collection, use and disclosure of personal information generally and, by extension, by AI-based solutions. That being said, both the federal

and provincial governments in Canada are developing a framework that is expected to include guidelines for organisations to use and procure AI-based solutions.

Effective in 2019, the government introduced the Directive on Automated Decision-Making (the "Directive"), the goal of which is to utilise AI when making, or planning to make, administrative decisions to improve service delivery in a way that is "compatible with core administrative law principles such as transparency, accountability, legality and procedural fairness". The Directive set out specific requirements which all government departments and ministries must adhere to when developing or procuring AI-based solutions, including providing notice in advance of any automated decision-making and ensuring that any such automated decision is accompanied by a meaningful explanation. In 2023, the government updated the Directive after soliciting stakeholder engagement. The updated Directive includes an expanded scope and new measures for bias testing, explanation, peer review, gender-based analysis plus, and data governance.

On 24th April 2023, AIDA, which focuses on regulating high-impact AI systems, was sent to parliament for consideration as part of Bill C-27. The substance of AIDA has been kept purposefully vague to allow for flexibility in adapting to rapid AI development. However, this lack of substance in AIDA has resulted in a fair amount of concern among stakeholders. Innovation, Science and Economic Development Canada has since released a companion policy that expands on the functionality of AIDA by helping to define what AI systems qualify as high impact. If an AI system qualifies as high-impact, AIDA states that the system operator must establish measures to identify, assess, and mitigate the risks of harm or biased output that could be created using said system. These specific measures are yet to be explicitly established, but the AIDA companion document provides useful guidance. If Bill C-27 is passed into law, the earliest the AIDA would likely be implemented is 2025.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

The increased prevalence of generative AI also raises a myriad of questions around copyright ownership. Canada does not currently have any laws that govern the ownership of data used to train machine learning-based systems. As a result, any contract between parties pertaining to the use of machine learning-based systems and the relevant data will need to specifically address the ownership rights of the respective parties. Until such time as the government introduces applicable legislation or the courts rule on a comparable situation, general contracting principles will apply.

Whether such data can be licensed commercially will depend on a number of issues, including the type and sensitivity of the data and the rights that each party might have in relation to the data, along with any sector-specific legislation or regulations that could apply to such data. However, presuming there are no explicit prohibitions arising due to the factual matrix, such data will generally be capable of being licensed commercially.

Recently, there have been complaints surrounding machine learning-based systems collecting, using, and disclosing users' personal information without their consent, in particular related to specific AI industry players. As a result of such complaints, in April 2023, the Office of the Privacy Commissioner ("OPC") announced it was opening an investigation into OpenAI and in May 2023, the privacy authorities from Quebec, British Columbia, and Alberta announced that they were joining the investigation. No new laws have been implemented in the face of these privacy concerns and investigations, but the OPC has released a reference guide on algorithmic fairness.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Ownership of the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer is not something that is specifically addressed under Canadian intellectual property legislation.

Canadian IP laws do not generally recognise a machine as the author (for copyright) or inventor (for patents). Instead, the presumption is that a human is the true author or inventor, not a machine.

These ownership questions are currently under review and the Canadian federal government is considering three approaches to determining the authorship and ownership of algorithms created by artificial intelligence: (i) the author is the human who arranged for the work to be created (via the machine); (ii) copyright can only apply to humans and therefore such algorithms would be authorless; or (iii) create new ownership rights for works generated by machines using artificial intelligence. The ultimate conclusion on ownership will be shaped by discussions currently ongoing within Canada and globally among government and key stakeholders on this issue.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

There are no national laws or regulations that specifically regulate the procurement of blockchain-based solutions. However, aspects of blockchain-based solutions may attract regulation under other frameworks (e.g., consumer protection laws, e-commerce legislation, securities laws, anti-spam legislation, intellectual property laws and privacy laws).

One of the most highly-regulated blockchain-based solutions is cryptocurrency. Canadian securities commissions have generally considered cryptocurrency assets, which are based on the blockchain, as "securities" which means that issuers distributing cryptocurrencies must comply with securities law obligations, subject to applicable exemptions.

In August 2022, the Canadian Securities Association ("CSA") established that unregistered crypto asset trading platforms operating in Canada must now sign a pre-registration undertaking ("PRU") addressed to their principal regulator that addresses various areas including investor protection. Then, in November 2022, the federal government announced its intention to conduct a legislative review on the stability of the financial and digital money sector and a consultation on digital currencies such as stablecoins and central bank digital currency. These recent announcements are expected to narrow the gap between regulated/unregulated crypto platforms operating in Canada.

Interestingly, in early 2022 the federal government imposed the *Emergencies Act* to clamp down on a trucker protest against COVID-19 vaccine mandates and, in so doing, approached the regulation and use of cryptocurrencies and blockchain technologies from a new and unique angle. Effectively, through its actions, the federal government showed that blockchain-based technologies are not as anonymous as many thought and the

result is that know-your-client processes and regulations will now likely begin to work their way into blockchain-based technologies more consistently.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

The widest use of blockchain solutions remains in financial services and fintech (crypto and digital currencies; identity verification for payments; transaction authentication). The payment and verification processes which are facilitated through blockchain, as well as other efficiencies which can be achieved through blockchain, have resulted in blockchain technologies being embraced by many industries including healthcare (vaccine supply chain integrity; vaccine passports), travel and mobility (car leasing; ride-hailing; airlines); telecommunications, legal (digital smart contracts), insurance, media and entertainment, supply chain management, manufacturing, logistics, transportation (car leasing and ride-hailing), gaming, retail and consumer packaged goods and government.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Parties considering procuring blockchain-based technologies will want to be weary of the legal uncertainty that accompanies any such emerging technology. As blockchain-based technologies continue to evolve and develop at an accelerated pace, legislators and regulators are unable to keep up from a regulatory perspective. Consequently, the legislative response is often outdated immediately upon any regulations or legislation coming into force because the technology has evolved.

One layer of uncertainty is that of classification and jurisdiction. As blockchain-based technologies emerge in the marketplace, we are generally left wondering what implications these technologies create at law (i.e., whether the technology is a security; whether it is a currency; whether it is captured by anti-money laundering regimes; which domestic or international bodies have jurisdiction over blockchain transactions, etc.).

Another legal complexity is the balancing act in a decentralised consumer protection dichotomy. While there are many benefits associated with decentralised data storage and multi-user verification access, these benefits come at the cost of concern surrounding data protection and cyber threats. Without robust regulatory frameworks in place, bad actors may leverage industry knowledge gaps to exploit users of blockchain-based technologies and/or bankroll illegal activities.

In addition, the ever-present issue of privacy and the protection of personal information that exists on the blockchain, and the fact that information on the blockchain may be broadly accessible (especially in public blockchain technologies) could result in violations of PIPEDA or the corresponding provincial privacy legislation. As a result, a detailed privacy impact assessment should be conducted by any organisation looking to utilise blockchain-based technologies in its services to ensure that it can comply with all privacy obligations and not put its customers' or other third parties' personal information at risk.

We anticipate new legal issues surfacing as blockchain use continues to evolve.

Robert Piasentin is the Group Head of the firm's Technology Law Group and is the Co-Head of the firm's Start-ups and Emerging Companies Group. Robert practises business and technology law with a focus on technology outsourcing transactions, software development and licensing solutions, strategic technology commercialisation arrangements, and privacy and cybersecurity issues. He has extensive experience working with clients in a range of industries, including technology, sports, and media, communications and entertainment. Earlier in his career, Robert served as the general counsel, corporate secretary and privacy officer for a leading information technology firm for more than 13 years.

McMillan LLP
Royal Centre, Suite 1500
1055 W. Georgia Street
Vancouver, British Columbia, V6E 4N7
Canada

Tel: +1 604 893 7636
Email: robert.piasentin@mcmillan.ca
URL: www.mcmillan.ca

Greg Johns is an accomplished business lawyer and highly skilled negotiator with a focus on the technology sector. His broad experience includes complex global contract negotiations and drafting, with a particular focus on infrastructure and application outsourcing and cloud computing. Prior to joining McMillan, Greg was one of IBM's senior legal executives. He structured and led the negotiation of some of IBM's largest and most complex long-term global contracts with large private and public sector customers, ranging from $100M to over $1B in value. Outside of Canada, Greg has worked on deals in the United States, UK, Mexico, Brazil and Asia.

McMillan LLP
Brookfield Place, Suite 4400
181 Bay Street
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 305 7187
Email: greg.johns@mcmillan.ca
URL: www.mcmillan.ca

Yue Fei is a member of the firm's Business Law Group and Technology Law Group, where she practises business, technology, and intellectual property law with a focus on technology related transactions, intellectual property and technology commercialisation arrangements, and privacy and data protection issues. She is also a registered trademark agent and a Certified Information Privacy Professional in Canada.

McMillan LLP
Royal Centre, Suite 1500
1055 W. Georgia Street
Vancouver, British Columbia, V6E 4N7
Canada

Tel: +1 236 826 3263
Email: yue.fei@mcmillan.ca
URL: www.mcmillan.ca

Anika Klassen is developing a broad business law practice that includes general corporate and commercial matters, sales and purchases of businesses and assets, and business structuring and organisation. Anika's practice also encompasses acquisition, commercialisation and enforcement of intellectual property rights. As a member of the firm's Technology Group, Anika is building expertise in advising startup and established companies as they navigate business needs in areas of technology outsourcing transactions, software development and licensing solutions, cybersecurity issues, and strategic intellectual property and technology commercialisation arrangements.

McMillan LLP
Royal Centre, Suite 1500
1055 W. Georgia Street
Vancouver, British Columbia, V6E 4N7
Canada

Tel: +1 236 826 3018
Email: anika.klassen@mcmillan.ca
URL: www.mcmillan.ca

McMillan is a leading business law firm serving public, private and not-for-profit clients across key industries in Canada, the United States and internationally. With recognised expertise and acknowledged leadership in major business sectors, we provide solutions-oriented legal advice through our offices in Vancouver, Calgary, Toronto, Ottawa, Montréal and Hong Kong. McMillan's Technology Law Group experts have a thorough understanding of legal and regulatory obligations related to technology, intellectual property, privacy, and cybersecurity, and regularly advise organisations with respect to technology outsourcing transactions, software development and licensing solutions, strategic intellectual property and technology commercialisation arrangements, and privacy and cybersecurity issues.

www.mcmillan.ca

mcmillan