Technology/E-Commerce

Doing Business in Canada

AIRD BERLIS

2026 EDITION

airdberlis.com

Canada has a thriving technology sector that supports key economic drivers, including technologies such as e-commerce, connected vehicles, artificial intelligence, cybersecurity, financial technology (including cryptocurrencies and other blockchain applications), medical technology, space and aviation technology, general software development, and many more. Since mid-2025, a number of cross-cutting regulatory developments have emerged. These include new federal oversight for certain financial technology activities, heightened anti-money laundering requirements, pending privacy law reforms, proposed artificial intelligence governance and initiatives targeting competition in digital markets and cybersecurity. These changes, outlined below, are poised to materially affect technology businesses operating in Canada. The legal framework governing the technology sector is shared by the federal and provincial governments. Commercial activity in technology involves multiple legal regimes, including intellectual property law (patents, copyrights, trademarks and trade secrets), broadcasting and telecommunications law, privacy and personal data security, consumer protection (e.g., oversight over deceptive marketing practices under the *Competition Act*), anti-spam (CASL), transportation and aviation safety regulation, import/export controls, confidentiality, education and health.

The scope of legislative and judicial jurisdiction over technology is in flux. In recent judicial decisions, the Canadian courts have shown a willingness to assume jurisdiction over non-Canadian businesses providing services in Canada even if they have no physical presence in Canada. Even "virtual businesses" may be found to be "carrying on business" in Canada.

PRIVACY AND DATA PROTECTION

Technology businesses in Canada continue to face an evolving privacy landscape. Federally, comprehensive reform of private-sector privacy law remains pending. In 2022, the government introduced Bill C-27 (*Digital Charter Implementation Act*), which was to enact a new *Consumer Privacy Protection Act* ("**CPPA**") to replace Canada's existing *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"). Among other changes, the CPPA would have imposed stronger accountability requirements, enhanced individual rights (e.g. algorithmic transparency, data mobility) and significantly larger penalties for non-compliance, enforced by a new Data Protection Tribunal. However, Bill C-27 did not become law: it progressed to committee in 2024 but died on the Order Paper in early 2025 due to the federal Parliament's prorogation and a snap election. There is cross-party consensus that PIPEDA is outdated and needs modernization, so reintroduced privacy legislation is expected at some point in the near future (likely with some adjustments to address concerns raised about the prior bill).

Until new federal legislation passes, organizations in Canada's tech sector must continue to comply with PIPEDA (as well as applicable provincial private-sector privacy laws).

Notably, the Province of Quebec has already enacted sweeping new privacy requirements. "Law 25" (previously Bill 64) came into force in stages by September 2023, imposing obligations such as mandatory privacy impact assessments for data transfers out of Quebec, privacy-by-default settings, data portability rights and corporate accountability measures (e.g. appointing a privacy officer and adopting a privacy policy) for any business handling Quebec residents' personal information. Law 25 also introduced some of the toughest penalties in Canada for privacy breaches, including fines up to the greater of $25 million or 4% of worldwide turnover for serious offences.

Other provinces (e.g., British Columbia and Alberta) are considering updates to their privacy statutes to follow suit. Technology companies should closely monitor these developments, as robust data protection compliance is increasingly becoming both a legal requirement and a business imperative in Canada.

ARTIFICIAL INTELLIGENCE

Canada's efforts to regulate AI saw significant activity in 2023-2025 but remain a work in progress. The centrepiece was the proposed *Artificial Intelligence and Data Act* ("**AIDA**"), introduced as Part 3 of Bill C-27. AIDA would have established a framework for "high-impact" AI systems, including baseline requirements for transparency, risk mitigation and human oversight, and prohibited AI use cases that cause serious harm (with potential fines for violations). The draft law contemplated an AI and Data Commissioner to monitor compliance.

Throughout 2023, AIDA underwent vigorous parliamentary debate and amendments (for example, narrowing definitions and shifting some enforcement powers from the minister to an independent commissioner). By late 2024, AIDA was still under committee review. In 2025, the legislative process was cut short: with the early-2025 dissolution of Parliament, Bill C-27 (and AIDA within it) died on

the Order Paper. Consequently, as of 2026, Canada currently has no comprehensive AI-specific statute in force. Enforcement initiatives are being pursued under existing statutory frameworks (including the *Competition Act* and applicable privacy laws), rather than under AI-specific legislation.

In June 2026, the federal government released Canada's National Artificial Intelligence Strategy, *AI for All*. The strategy represents a significant evolution in Canada's approach to AI policy, shifting from a singular legislative focus (as reflected in AIDA) to a broader, co-ordinated framework combining economic policy, infrastructure investment and targeted regulatory initiatives. It is structured around national priorities including protecting Canadians and democratic institutions, expanding AI literacy and workforce readiness, accelerating adoption across the economy, building Canadian-controlled ("sovereign") AI infrastructure, scaling domestic AI companies and strengthening international partnerships. These priorities reflect the federal government's objective of positioning AI as a general-purpose technology that drives productivity and economic growth.

Accordingly, businesses operating in Canada should anticipate that current policy commitments under the *AI for All* strategy may translate into binding legal requirements over time. In particular, organizations deploying AI systems should be prepared to align their practices with emerging expectations around transparency, accountability, data governance, risk assessment and human oversight, even in advance of formal statutory obligations.

In the meantime, businesses deploying AI in Canada should be aware of sector-specific guidelines and emerging best practices. For example, the federal government has endorsed voluntary codes of conduct for AI, and regulators such as the federal and provincial Privacy Commissioners and the Competition Bureau have signaled vigilance on AI-related privacy abuses and anti-competitive behaviour. Indeed, the Competition Bureau's 2025-26 plan explicitly made "artificial intelligence" a priority sector for enforcement (e.g. scrutinizing AI-enabled anti-competitive conduct).

Companies seeking to do business in Canada should anticipate future mandatory AI requirements and consider instituting internal AI governance measures (bias testing, transparency, human-in-the-loop oversight for high-impact automated decisions) in preparation for the coming regulatory framework.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE

With cyber threats on the rise, Canadian authorities have advanced initiatives to protect critical digital infrastructure, though comprehensive legislation remains pending. In mid-2022, the federal government introduced Bill C-26, the *Critical Cyber Systems Protection Act* ("**CCSPA**"), which would have imposed baseline cybersecurity and breach reporting obligations on operators in key sectors (including telecommunications, finance, energy, transportation and other vital systems). The CCSPA would have empowered the government to designate "vital services and systems" and require their operators to establish cybersecurity programs, report incidents and comply with cyber standards, with oversight by national security agencies.

Additionally, Bill C-26 proposed to amend the *Telecommunications Act* to explicitly authorize the government to bar high-risk suppliers and otherwise "secure the Canadian telecom system." By late 2024, Bill C-26 had progressed through much of the legislative process, including Senate amendments. However, like other bills, it was halted by the 2025 federal election call and did not become law.

It is widely expected that a similar cybersecurity bill will be reintroduced, given bipartisan recognition of the need to protect critical infrastructure. In the interim, the government has used other tools to address urgent risks. For example, it has directed telecom companies to remove certain foreign equipment from 5G networks and launched a voluntary Cyber Security Certification Program for smaller businesses.

Companies in sensitive sectors should follow guidance from the Canadian Centre for Cyber Security, which has published baseline cyber controls and sector-specific advisories. Several provinces have started to incorporate cybersecurity obligations into critical infrastructure regulation (for instance, Ontario's energy sector cybersecurity framework).

Until a comprehensive federal law is in place, regulators and industry bodies are increasing expectations around cyber preparedness, including regular risk assessments, incident response plans and direct involvement of boards in cyber oversight. Tech companies, especially those providing services in areas such as cloud computing, fintech or health tech, should be prepared for more rigorous cybersecurity compliance requirements in the near term and ensure that their systems align with established best practices and standards.

COMPETITION AND DIGITAL MARKETS

The competition law environment in Canada has undergone notable changes aimed at digital commerce and big tech practices. Amendments in 2022 and 2023 strengthened the federal *Competition Act* in ways that affect tech businesses. For example, Canada outlawed certain forms of "drip pricing" (hidden fee tactics often seen in online sales) as a deceptive practice and significantly increased Administrative Monetary Penalties for anti-competitive conduct and deceptive marketing (now up to 3% of a firm's global revenue or more in some cases).

Mergers that may lessen competition, including in digital markets, now face more stringent review, as lawmakers removed the statutory "efficiencies" defence through amendments introduced in 2022 and brought into force subsequently, giving the Competition Bureau greater leverage. In December 2023, new provisions granted the Bureau the ability to conduct market studies using court orders to compel information from firms, a power intended to support investigations into digital platform dominance.

The Bureau has signaled an increasingly assertive stance. In its 2025-26 annual plan, it highlighted a "new era of competition enforcement" and identified digital sectors (including online platforms, data and artificial intelligence) as enforcement priorities.

The federal government has also been examining the need for *ex ante* regulation of large digital platforms (sometimes referred to as a "Digital Markets Act" approach), though as of 2026 no such legislation has been tabled.

Technology companies should nonetheless be mindful of the Competition Bureau's proactive approach. This includes increased scrutiny of tech mergers, greater focus on how dominant firms handle consumer data (with data portability and interoperability on the Bureau's radar) and crackdowns on misleading digital marketing, including influencer advertising and greenwashing claims for tech products.

In sum, the competition law framework is evolving to address the challenges of the digital economy, and tech businesses must ensure their practices withstand heightened regulatory scrutiny.

FINTECH, PAYMENTS AND CRYPTOCURRENCIES

Significant regulatory changes between 2025 and 2026 have introduced new oversight for financial technology and payment services.

Anti-Money Laundering and Financial Services Regulation

Canada's anti-money laundering ("**AML**") regime was expanded effective April 1, 2025. Businesses engaged in financing or leasing are now explicitly regulated as reporting entities under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. This brings many equipment financing, leasing, factoring and cheque-cashing companies under FINTRAC supervision, requiring compliance programs including client identity verification, record-keeping and transaction reporting similar to those required of banks.

These new AML obligations were accompanied by enhanced Canada Border Services Agency powers to combat trade-based money laundering and new beneficial ownership discrepancy reporting rules coming into force in October 2025. FINTRAC has indicated an initial focus on outreach and implementation support, followed by stricter enforcement beginning April 1, 2026.

Retail Payments Oversight

Canada's first federal retail payments framework is now in force under the *Retail Payment Activities Act* (enacted in 2021) and final regulations published in November 2023. By November 2024, all non-bank payment service providers ("**PSPs**") were required to register with the Bank of Canada.

As of September 8, 2025, substantive requirements fully took effect. Registered PSPs must maintain risk management programs, safeguard end-user funds in trust or through insurance and comply with annual reporting and incident notification obligations. The Bank of Canada now supervises roughly 1,500 PSPs and maintains a public registry of registered and refused entities. This new regime brings fintech payment platforms, money transfer apps, digital wallets and similar services under a national oversight framework for the first time.

Crypto Assets and Stablecoins

Canada is moving toward a more formalized framework for crypto assets, particularly stablecoins. In late 2025, the federal government announced plans for legislation to regulate stablecoin issuers, including requirements for reserve assets,

redemption rights and risk management. The proposed framework would designate the Bank of Canada as the regulator for qualifying stablecoins and amend the *Retail Payment Activities Act* to clarify that certain stablecoin activities remain within payments oversight rather than securities law.

As of early 2026, this legislation has not yet been introduced. In the interim, the Canadian Securities Administrators ("**CSA**") continue to treat many fiat-backed stablecoins as "value-referenced crypto assets" that may fall under securities or derivatives regulation. Since 2024, the CSA has required crypto trading platforms to cease trading in certain stablecoins or obtain enhanced undertakings from issuers pending this new federal regime.

More broadly, the federal government has renewed its focus on Open Banking (consumer-directed banking). After years of consultation, Budget 2025 committed to advancing Open Banking by introducing a Consumer Data Right and a "Consumer-Driven Banking Act." The initiative would enable individuals and businesses to securely share banking data with fintechs and initiate payments through third-party providers by 2026 or 2027. Oversight is expected to shift to the Bank of Canada from the Financial Consumer Agency of Canada, aligning Open Banking with the new payments supervision regime. This initiative, still in development, is expected to increase competition and innovation in financial services, and intersects with privacy through a planned data mobility right under federal privacy reform.

Crypto Regulation Framework

The treatment of crypto assets in Canada depends on whether they are classified as securities or derivatives, which is crucial to determine the applicable legal framework. If so classified, they become subject to prospectus requirements, dealer and adviser registration, disclosure and reporting rules, custody standards and investor protection measures. The analysis typically arises at both the issuance stage (including initial coin offerings (ICO)) and during trading on crypto asset trading platforms.

Securities regulators have also begun to differentiate between types of crypto assets, such as stablecoins, utility tokens and governance tokens, applying different analyses depending on their function.

While cryptocurrencies are not considered legal tender, it is not generally illegal to receive or possess them in Canada. However, trading in cryptocurrencies is regulated where transactions occur through a "crypto asset trading platform" – an online marketplace that enables users to transfer, hold and exchange various crypto assets. These platforms are required to register and comply with applicable regulatory requirements, and failure to do so may result in significant penalties. They are also subject to standard anti-money laundering and know-your-client rules applicable to securities market participants.

The term "value-referenced crypto asset" commonly refers to stablecoins. According to the CSA, these assets are designed to maintain a stable value by referencing fiat currency or other underlying assets, and are backed by reserves or linked to non-fiat assets. Depending on their structure, value-referenced crypto assets may be classified as securities and/or derivatives.

The CSA has introduced regulatory guidance applicable to issuers and registered crypto asset trading platforms dealing in trading value-referenced crypto assets. The guidance includes expectations to engage with regulators, provide undertakings for fiat-backed stablecoins and cease offering certain products where required. Additional obligations include compliance with prescribed disclosure requirements, disclaimers and updated policies effective as of April 30, 2024.

The Canada Revenue Agency, Canada's taxation authority, treats cryptographic tokens (including cryptocurrencies) as commodities for taxation purposes, triggering various kinds of tax obligations depending on the circumstances.

IMPORT/EXPORT CONTROLS

Importing certain technologies into Canada may obligate importers to comply with requirements under the *Defence Production Act* (Canada), the *Controlled Goods Regulations* (Canada), the *Export and Import Permits Act* (Canada), as well as the U.S. International Traffic in Arms Regulations (ITAR) and the U.S. Export Administration Regulations, the latter of which are both "long arm" laws that extend beyond the borders of the United States into Canada. The Controlled Goods Program, which is governed under the Controlled Goods Regulations, is mandated to protect goods and/or controlled technologies within Canada that have a military application or a national security significance, and to prohibit such controlled goods and/or technologies from being accessed by unauthorized persons or exported/re-exported to certain countries. In practice, Canadian companies operating in cross-border supply chains often face overlapping and

sometimes competing obligations under Canadian and U.S. export control regimes. This requires careful contractual and compliance structuring to ensure that obligations under foreign laws are observed without contravening applicable Canadian law. It is common to include express limitations stating that compliance with foreign export controls will be undertaken only to the extent permitted by Canadian law.

Canada's export control regime is regulated by multiple domestic laws, international agreements and diplomatic obligations, including an Export Control List. Export permits may be required not only to ship goods outside Canada, but to provide services associated with designated technologies, discuss designated technologies with certain employees of non-Canadian citizenship, participate in phone or video conversations about designated technologies, correspond by email, fax or otherwise through cyberspace about designated technologies, and sometimes even before leaving Canada's borders on business trips. Factors such as the nature, characteristics, origin of componentry, intended uses, destination and end users of the technology are all relevant to whether an export permit is required.

In 2018, Canada introduced the Brokering Control List to comply with the Arms Trade Treaty. This list identifies specific goods and technology that require a brokering permit. The permit authorizes the arranging or negotiation of transactions leading to the movement of controlled goods and technology between two foreign nations.[1]

The Area Control List is a list of countries for which export permits are required for any goods and technology exported from Canada, regardless of whether such goods and technology are on the Export Control List. As of this writing, the only country on Canada's Area Control List is the Democratic People's Republic of Korea (i.e., North Korea).[2]

U.S. companies working with businesses in Canada should be mindful of areas of conflict between Canada's export control laws and U.S. export control laws. Canadian companies should be mindful that compliance with certain foreign extraterritorial measures (particularly those relating to U.S. sanctions against Cuba) may, in limited circumstances, conflict with Canadian law. Under the *Foreign Extraterritorial Measures Act* and related orders, Canadian entities may be prohibited from complying with specified foreign measures where such compliance would contravene Canadian public policy. However, in practice, Canadian businesses frequently comply with U.S. export control regimes (including ITAR and the Export Administration Regulations), subject to appropriate contractual carve-outs (e.g., compliance "to the extent permitted by applicable law") to manage potential conflicts.[3] For this reason, Canadian counsel will often advise their Canadian clients agree to comply with such U.S. laws only to the extent permitted by applicable law or by the laws of Canada.

In addition, under the *Foreign Extraterritorial Measures (United States) Order, 1992*, a Canadian corporation and its directors, officers, managers or employees may be prohibited from complying with any extraterritorial measures imposed by the U.S. against Cuban businesses. In this regard, entities must be cognizant around directives, instructions or communications related to such relationships received from individuals who hold influence over the Canadian corporation's policies within Canada. This prohibition extends to any act or omission that amounts to compliance with U.S. extraterritorial legislation concerning Cuba, irrespective of whether such compliance is the sole intent behind the action or omission.[4]

E-COMMERCE STATUTES

Subject to a few exceptions, Canada's federal government and the Canadian provinces have adopted electronic commerce statutes that deal with issues arising from conducting business electronically. For example, Ontario legislates elements of e-commerce under the *Electronic Commerce Act*, while this area is also subject to the federal *Personal Information Protection and Electronic Documents Act*. Canada's e-commerce statutes typically set out standards for the use of enforceable electronic signatures and establish requirements for documents that would otherwise have to be in writing to be valid in electronic form. In some provinces – for example, Quebec – there are special rules applicable to consumers that pertain to both format/appearance and the language used that affect the enforceability of an electronic document. These e-commerce statutes also set forth how and when an offer and acceptance of a contract distributed electronically may be made – provisions that may not neatly align with the *United Nations Convention on Contracts for the International Sale of Goods* (CISG).

1 Brokering Controls (international.gc.ca)

2 https://laws-lois.justice.gc.ca/eng/regulations/SOR-81-543/index.html

3 Foreign Extraterritorial Measures Act (FEMA)

4 Foreign Extraterritorial Measures (United States) Order, 1992 (justice.gc.ca)

INSOLVENCY

Canadian bankruptcy and insolvency laws underwent revisions in 2009 and 2019 to afford greater protection to contractual users of intellectual property (including technology-related intellectual property). Amendments made to the bankruptcy, insolvency and restructuring laws in 2019 provided some clarity on the impact of intellectual property sales or dispositions in the context of bankruptcy, receivership or restructuring. The goal was to ensure that the bankruptcy, insolvency or restructuring of a company that grants rights to use intellectual property does not wholly impede the grantee's rights to use that intellectual property, provided the grantee continues to make all required payments and fulfill all other contractual obligations. However, if the bankrupt or insolvent company exercises its right to "disclaim" the original contract, the user cannot expect to continue to receive support, updates or other benefits from the intellectual property owner under that contract.

Canadian insolvency legislation (including the *Bankruptcy and Insolvency Act* and the *Companies' Creditors Arrangement Act*) provides statutory protection for a licensee's continued right to use intellectual property notwithstanding a disclaimer or assignment of the underlying agreement, provided that the licensee continues to perform its obligations. Canadian courts have generally upheld this "right to use" as a meaningful protection for licensees. However, uncertainty remains regarding the precise scope of that right, particularly with respect to ancillary rights (such as access to updates, support services or SaaS-type arrangements), as the legislation does not comprehensively define the scope of the protected "right to use." While one may assume that all statutory intellectual property rights are protected, Canada also recognizes common law intellectual property rights in trademarks and trade secrets. The insolvency legislation provides no guidance as to what constitutes the "right to use" (the particular right that is protected). Because the legislation does not obligate a bankrupt grantor of a "right to use" intellectual property to continue providing maintenance or support, the benefit of the provision must be regarded as limited.

On the other side of the coin, there is little, if any, protection for a licensor should its licensee become insolvent. Serious consequences may arise for licensors of valuable, limited-use intellectual property due to the broad authority of Canadian courts' right to assign licence agreements to third parties in insolvency proceedings, particularly where the market for such licences is limited. In effect, the insolvency of a licensee could cost the licensor a new sale if the licensee's bankruptcy trustee is willing to sell the licence for less than the original licensor is charging.

APPLICABILITY OF SALE OF GOODS LEGISLATION

In Canada, certain rights and obligations will follow the acquisition or sale of technology that falls within the scope of provincial sale of goods legislation. Canadian courts tend to treat computer system acquisitions as sales of goods while transactions involving pure service, maintenance, training or programming are typically viewed as incidental to the sale of goods and therefore not subject to sale of goods legislation – and therefore not subject to the statutory protections contained in such legislation. Software supplied solely pursuant to a licence agreement is generally not subject to sale of goods legislation, particularly where no transfer of property occurs. However, Canadian courts assess such arrangements on a fact-specific basis, and transactions involving bundled hardware and software or other hybrid arrangements may be characterized differently.

LIBEL ACTION OVER THE INTERNET

Cyber-libel is the posting of defamatory statements made online – such as through social media, blogs, emails or websites – that harm a person's reputation. To establish a claim for defamation in Canada, a plaintiff must demonstrate that the impugned statement is defamatory in nature, that it refers to the plaintiff and that it has been published to at least one third party. Falsity and malice are not required elements of the cause of action, although malice may be relevant in defeating certain defences (such as qualified privilege) and in assessing damages. Canadian courts have generally treated online communications (including emails, blogs and website content) as publications for the purposes of defamation law, rather than traditional "broadcasts." However, the application of limitation periods can be context-specific, and issues may arise in respect of republication, discoverability and timing of online dissemination. As information on the internet is widely disseminated in a short period of time, there is a high probability of significant damages resulting from a cyber-libel.

An issue that has arisen in the context of cyber-libel is the anonymous posting of defamatory statements or images to the internet, including AI-generated images (discussed below) that are defamatory in nature. Certain jurisdictions in Canada have privacy

statutes that make it a tort to violate someone's privacy, including using someone's likeness or image without consent, especially if it causes harm or is used for commercial gain.

Although it is possible to obtain early mandatory orders or discovery from third parties that allow one to learn the identity of a cyber-libeller, it is often an expensive exercise. In addition, this information may not prove to be useful since the publisher may have posted the defamatory statement or image from an internet café or other public resource that does not keep records of its users.

In the United States, internet service providers ("**ISPs**") are generally protected from liability in respect to the content of others. In Canada, such immunity is less clear-cut.

CYBERBULLYING/REVENGE PORN

Amanda Todd, a young teenager, was a Canadian victim of cyberbullying. It was determined that she had been extorted by one Aydin Coban, a resident of the Netherlands, into indecently exposing herself, and she ultimately committed suicide. Coban was tried and convicted in Canada and is currently serving a 13-year prison term in Canada. As a result of the bullying suffered by Todd and her subsequent suicide, the Canadian federal government passed the *Protecting Canadians from Online Crime Act* (Canada), now part of the Canadian *Criminal Code*. It created the criminal offence of non-consensual distribution of intimate images (revenge porn) and has been in force since March 2015.

If an AI-generated image falsely implies misconduct or damages a person's reputation, it may be considered defamatory. Further, the surge of generative artificial intelligence platforms and technologies, like deepfakes, has aggravated the menace of revenge porn and cyberbullying, making it easier for individuals with malicious intent to create and distribute manipulated content without the consent of the victims. Most Canadian provinces have enacted specific legislation addressing the non-consensual distribution of intimate images. Ontario has not adopted a standalone statute of this nature, instead relying primarily on general criminal law provisions and civil remedies, including privacy torts such as intrusion upon seclusion and existing statutory causes of action. British Columbia is the latest province to enact the *Intimate Images Protection Act*, which came into force in January 2024. It applies retroactively to March 6, 2023. The Act created new civil rights and remedies, including an expedited process for a person whose intimate images have been distributed without consent or who has received threats of such distribution, to swiftly seek orders to stop and prevent the spread of these images.[5]

.CA DOMAIN NAMES

Internet domain names are verbal representations of numerical addresses used to identify and locate websites on the internet. Each internationally recognized country is entitled to one top level domain ("**TLD**"), referred to as a country code top level domain, or ccTLD. Canada's ccTLD is the .ca domain. The .ca domain is currently administered by the Canadian Internet Registration Authority.

Registration in the .ca domain is available only to applicants who can demonstrate Canadian presence requirements, namely, Canadian citizens, permanent residents or their legal representatives, Aboriginal peoples,[6] corporations incorporated under the laws of Canada or any province or territory, foreign corporations with an extra-provincial licence to operate in Canada, trusts, partnerships, associations and other individuals and entities that meet certain requirements. Generally, the registration and transfer processes for .ca domain names are not particularly sophisticated or complicated. Dispute resolution processes in the .ca domain were established in 2001.

ASSIGNING AND SUBLICENSING TECHNOLOGY LICENCES

Under Canadian law, the assignability and sublicensability of a technology or software licence depends on the nature of the licence and the intentions of the parties. In the absence of express contractual language, Canadian courts assess whether the licence is "personal" to the licensee (meaning that it was granted in reliance on the identity, skill, financial capacity or particular circumstances of that licensee). Where a licence is found to be personal in nature, it is generally not assignable or sublicensable without the licensor's consent. This principle reflects the common law rule that contractual rights involving personal confidence or discretion cannot be transferred unilaterally. Conversely, where a licence is non-exclusive, broadly framed and does not involve a close or trust-based relationship, courts are more likely to treat it as assignable, subject to any express contractual restrictions.

5 Intimate images and consent - Government of British Columbia (gov.bc.ca)

6 Canadian Presence Requirements – CIRA

Express provisions in the licence agreement are determinative. Canadian courts will give effect to clear language permitting or prohibiting assignment and sublicensing, including clauses that require licensor consent, restrict assignment to affiliates or to a change of control, or deem certain transactions (such as amalgamations or asset sales) to constitute assignments. In the absence of a sublicensing right, a licensee generally has no implied right to grant sublicences, particularly where doing so would expand the class of users or undermine the licensor's control over its intellectual property. Accordingly, licensors typically address assignment and sublicensing expressly to preserve control over downstream use of their technology, while licensees should ensure sufficient flexibility is built into the agreement to accommodate corporate reorganizations, financings, outsourcing arrangements and exit transactions.

ENFORCEABILITY OF SHRINK-WRAP, CLICK-WRAP, AND BROWSE-WRAP LICENCES IN CANADA

The key for enforceability of shrink-wrap, click-wrap and browse-wrap agreements is whether or not it can be established that both parties to the contract were aware of the terms of the agreement and agreed to them. Canadian courts have tended to prefer forms of agreements where the terms of such agreement are brought to the attention of the person, with the person having to click "I Accept" prior to being bound to such terms, over those forms of agreement where the person is bound by the terms as a result of simply landing on a website. Accordingly, browse-wrap licences are generally more difficult to enforce and are typically avoided in favour of click-wrap or other mechanisms that clearly demonstrate user acceptance.

USE OF NON-CANADIAN FORM AGREEMENTS IN CANADA

Foreign technology companies that wish to use their standard commercial precedents to carry on business in Canada should ensure that certain "Canadian-specific" legal issues have been addressed in the form of agreement which is to be used. Some of these issues include the following:

Sale of Goods Act Conditions: Canadian practice relating to technology agreements is to ensure that any disclaimer of implied warranties contained in a technology agreement also disclaims the implied conditions imposed by sale of goods legislation.

Ownership Rights: Canadian law does not recognize the concept of "work made for hire," which is a phrase often contained in U.S.-based agreements. In a software scenario, typically, the author of a computer program is the first owner of copyright in the program. If the author is employed for the purpose of creating software, then the employer will generally be the first owner of copyright in the software. The law is similar for inventions and trade secrets. In situations where a copyright-protected work is created expressly for a customer by a contractor, the contractor, as author, will own the work unless the contractor has entered into a written assignment of copyright in favour of the customer. It is also standard practice in Canada to have such a written assignment accompanied by an express waiver of moral rights in the work.

These are in addition to the inclusion of appropriate clauses addressing specific Canadian regulatory matters, such as privacy, data security, anti-spam and any pending laws governing the use of artificial intelligence (including the formerly proposed federal *Artificial Intelligence and Data Act*, which was not enacted).

CONNECTED AND AUTONOMOUS VEHICLES

Connected vehicles are motor vehicles that can send and receive messages to and from other connected vehicles and roadside infrastructure. Those messages may pertain to time, place and distance of the connected vehicle and may contain road safety and awareness information. The intention is to allow users to drive on Canadian roads more safely.

Certain jurisdictions in Canada follow the standards for driving automation levels established by the Society of Automotive Engineers International, ranging from Level 0 (no automation) to Level 5 (full automation). As with motor vehicle transportation in general, regulation of autonomous or automated vehicles in Canada involves the federal, provincial/territorial, and municipal governments.

In 2024, Transport Canada released its *Safety Framework for Connected and Automated Vehicles 2.0*. The guidelines contained in that publication aim to establish a baseline of consistent best practices across provinces and territories for automated and connected driving systems, subject to Canada's *Motor Vehicle Safety Act*. [7] The framework outlines policies and instructions for the use of connected and automated vehicles (CAVs) on Canada's public

7 https://laws-lois.justice.gc.ca/eng/acts/M-10.01/

roads. It outlines the regulatory and oversight regime, including non-regulatory guidance for cybersecurity and testing, and details upcoming changes to the *Canada Motor Vehicle Safety Standards* (CMVSS) to accommodate Advanced Driver Assistance Systems (ADAS), Vehicle-to-Everything (V2X) communication and cybersecurity and data privacy protections.

Thanks to enabling legislation and interest in various municipalities, Canada is currently regarded as being advanced in technologies pertaining to connected and autonomous vehicles, as well as their testing and use.

June 2026

AIRD BERLIS

We are committed to being the Canadian gateway for our clients.

Brookfield Place, 181 Bay Street, Suite 1800, Toronto, ON M5J 2T9
T 1.416.863.1500 F 1.416.863.1515

701 West Georgia Street, Suite 1420, Vancouver, BC V7Y 1E4
T 778.371.2241 F 778.371.2270

Other articles and papers written by our professionals can be viewed at:

airdberlis.com

Doing Business in Canada offers general comments on legal developments of concern to businesses, organizations and individuals, and is not intended to provide legal opinions. Readers should seek professional legal advice on the particular issues that concern them.