



Technology/E-Commerce

Doing Business in Canada

AIRD BERLIS



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. 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.

TECHNOLOGY

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.

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.² 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).³

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.⁴ For example, Canadian companies may be subject to fines and other penalties should they agree to be bound by U.S. export control laws. For this reason, Canadian counsel will often have 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 other countries, such as U.S. embargoes 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

¹ Brokering Controls (international.gc.ca)

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

³ Area Control List (justice.gc.ca)

⁴ [Foreign Extraterritorial Measures Act \(FEMA\)](#)

legislation concerning Cuba, irrespective of whether such compliance is the sole intent behind the action or omission.⁵

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*.

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.

It is unclear which intellectual property rights enjoyed by users are protected from being disclaimed. 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.

.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.

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

⁵ Foreign Extraterritorial Measures (United States) Order, 1992 ([justice.gc.ca](https://www.justice.gc.ca))

⁶ [Canadian Presence Requirements – CIRA](#)

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 typically not subject to sale of goods legislation unless some sort of property is transferred to the licensee. If software is provided together with hardware or other goods (e.g., as a “system”), the software may become subject to sale of goods legislation.

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. The post has to be false and malicious. It is still unclear in Canadian jurisdictions as to whether email, blogs and the content of websites constitute a broadcast for the purposes of defamation law. If they do, short limitation periods may apply. 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, with the notable exception of Ontario, have enacted specific legislation to tackle this menace. 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.⁷

Assigning and Sublicensing Technology Licences

For a software licence to be assignable, the Canadian courts look to whether or not the licence is “personal” to the licensee. If a court determines that a licence is personal, the licence may not be assignable or capable of being sublicensed to third parties, subject to any language in the licence to the contrary.

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 best avoided.

⁷ [Intimate images and consent - Government of British Columbia \(gov.bc.ca\)](https://www2.gov.bc.ca/gov/content/industry/tech-innovation/ai-intellectual-property/intimate-images-consent)

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 to address specific Canadian regulatory matters, such as privacy, data security, anti-spam and any laws (currently under discussion) governing the use of artificial intelligence.

Cryptocurrencies

The chief legal concern arising from crypto assets in Canada is whether they qualify as securities or derivatives, which is crucial to determine the applicable legal framework. If they are found to be securities or derivatives, they become subject to prospectus requirements, dealer and adviser registration, disclosure and reporting requirements, custody requirements and investor protection measures. The determination of whether securities law applies to crypto assets typically arises in two distinct scenarios: during the initial coin offering (ICO) of these assets and their trading on crypto asset trading platforms. Further, securities regulators have 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 will be regulated if crypto trades are accomplished through a “crypto asset trading platform” – an online market that offers users the ability to transfer, hold and exchange various crypto assets. Failure of these online markets to register and comply with regulations attracts significant penalties. Crypto asset trading platforms are subject to the usual anti-money laundering and “know your client” rules by which all securities traders are bound.

The term “value-referenced crypto asset” commonly refers to stablecoins. According to the Canadian Securities Administrators (“CSA”), stablecoins can replicate the value of a single fiat currency and are backed by reserves of assets in that currency, or they can be non-fiat-backed stablecoins pegged to assets other than fiat currency. A value-referenced crypto asset is designed to maintain a stable value over time by referencing the value of a fiat currency, or any other value, right or combination thereof. The CSA considers value-referenced crypto assets as potentially being categorized as securities and/or derivatives.

The CSA has introduced regulatory guidance targeting issuers and registered crypto asset trading platforms involved in trading value-referenced crypto assets. The guidance includes requirements to contact regulators, provide undertakings for fiat-backed stablecoins and cease offering of certain value-referenced crypto assets. Additional obligations include compliance with prescribed disclosures, disclaimers and updated policies in effect as of April 30, 2024.

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.

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*.⁸ The framework outlines policies and instructions for the use of connected and automated vehicles (CAVs) on Canada's public 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 2025

⁸ <https://laws-lois.justice.gc.ca/eng/acts/M-10.01/>

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.

© 2025 Aird & Berlis LLP

Parts of this booklet may be reproduced with acknowledgment.
