



Technology/E-Commerce

2023

Doing Business in Canada

AIRD BERLIS

airdberlis.com

Canada has a thriving technology sector that supports key economic drivers, including such technologies as e-commerce, connected vehicles, artificial intelligence, cybersecurity, financial technology, 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 as it relates to the internet (copyright and trademarks), broadcasting and telecommunications law, privacy and personal data security, consumer protection (e.g., the oversight over deceptive marketing practices under the *Competition Act*), anti-spam (CASL), transportation and aviation safety regulation, import/export controls, confidentiality and trade secrets, 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 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) and even 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 and to prohibit controlled goods and/or controlled technology from being accessed by unauthorized persons.

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 to not only ship goods outside Canada, but to provide services associated with designated technologies, discuss designated technologies with certain employees, 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, uses to be made of the technology, destination and end users of the technology are all relevant to whether an export permit is required.

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. For example, Canadian companies may be subject to fines and other penalties should they agree to be bound by U.S. export control laws. In addition, directors and officers may face penalties under Canadian law for complying with any instruction by, or policy of, a U.S. entity, contrary to Canada’s policies relating to the trading between Canada and Cuba.

E-commerce Statutes

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 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 to be met in order to use an enforceable electronic signature and requirements to be met in order for a document 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 appearance and language used that affect enforceability of the document. These e-commerce statutes also set forth how and when an offer and acceptance of a contract distributed electronically may be made.

Insolvency

Canadian bankruptcy and insolvency laws underwent revisions in 2009 to afford greater protection to contractual users of technology (and other intellectual property). One of the key terms set forth in Canadian bankruptcy and insolvency legislation is that insolvent parties are generally permitted to “disclaim” (terminate) an agreement for the use of intellectual property, subject to the right in the counterparty to continue to use the intellectual property, provided that the user continues to make all payments and to carry out all user obligations called for in the original agreement. Of course, because of the exercise of

the disclaimer, the user cannot expect to continue to receive support, updates and other benefits from the insolvent intellectual property owner.

It is unclear which intellectual property rights enjoyed by intellectual property users are protected from being disclaimed. While one may assume all statutory intellectual property rights would be protected, Canada also protects common law intellectual property rights for trademarks and trade secrets. The insolvency legislation provides no guidance as to what the “right to use” (which is afforded protection) means. As mentioned, the legislation does not obligate the licensor to continue to provide maintenance or support should the licensor become insolvent.

On the other side of the coin, there is little, if any, protection for a licensor should its licensee become insolvent. There can be serious consequences for the licensor of valuable, limited use intellectual property arising from the Canadian courts’ broad right to assign licence agreements to third parties in the event of an insolvency. Imagine, for example, the insolvency of a chartered Canadian bank (of which there are few in Canada). A licence of software that is solely dedicated and useful to banks could be assigned to another bank without the concurrence of the licensor, depriving the licensor of a potential sale to the assignee.

.ca Domain Names

Internet domain names are verbal representations of a numerical address 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, corporations incorporated under the laws of Canada or any province or territory of 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 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 posting a statement or image on the internet which tends to lower the reputation of a person in the community. 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. Although it is possible to obtain early mandatory orders or discovery from third parties that allow one to learn the identity of the 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. While the law in jurisdictions within North America vary by province or state, as a result of a recent Supreme Court of Canada decision, the law in Canada is now closer to that generally applicable in the United States. In Canada, those who post statements and images which are false and defamatory may escape liability if they can demonstrate that the material was published responsibly.

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.

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 Todd's bullying and 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 2014.

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 parties. If the courts determine that a licence is personal, the licence may not be assignable or capable of being sublicensed to third parties, barring 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 the 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.

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 a "work made for hire," which is a phrase often contained in U.S.-based agreements. In a software scenario, typically, the author of the 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 a situation in which a copyrighted work is being created for a customer by a contractor, the contractor, as author, will be the owner of the work unless the contractor has entered into a written assignment of such 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.

Cryptocurrencies

From the legal point of view, cryptocurrencies in Canada are not generally illegal to receive or possess. However, trading in cryptocurrencies is regulated if the trades are accomplished through a "crypto asset trading platform" - a kind of online market that permits cryptocurrency exchanges. Failure to register and submit to regulation 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.

So-called "stablecoins" (cryptographic currencies that are supported by established fiat currencies like the U.S. dollar) are considered to be part of a class of securities called derivatives and are regulated as securities. At present, securities regulators in Canada are not licensing trading platforms that propose to deal in stablecoins or that offer margin accounts to traders in cryptographic currencies.

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.

Transport Canada, the federal regulator in Canada, has published a National Policy Framework for Connected and Automated Vehicles that encourages the promotion of the technology, including sensors, telecommunication and real-time positioning of vehicles that allow drivers to "see around corners" and learn of dangers that cannot otherwise

be known on the road. The regulator has also published a Safety Framework for Automated and Connected Vehicles that provides relevant guidance to manufacturers. These publications recognize that road accidents will still happen but that new technologies are likely to make such accidents far less frequent than currently is the case.

The relevant legislation is the *Strengthening Motor Vehicle Safety for Canadians Act* (Canada). That legislation allows for the speedy suspension or modification of existing laws to allow alignment with laws in force in other countries, especially the United States, since it is seen that safety depends in part on a uniform driving experience, no matter in which country a person is driving.

As for testing of autonomous vehicles, the Province of Ontario has permitted testing on Ontario roads (subject to certain caveats) since 2016, and Transport Canada has published guidelines for best practices for such testing.

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 2023

AIRD BERLIS

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



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

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.

© 2023 Aird & Berlis LLP

Parts of this booklet may be reproduced with acknowledgment.
