International
Comparative
Legal Guides

Digital Business 2020

A practical cross-border insight into digital business law

First Edition

ICLG.com

Canada

ROBIC LLP

Jean-François Normand

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

In Canada, e-commerce is regulated at both the federal and provincial level, with legislations varying widely on certain specific issues, while being generally consistent in their treatment of the enforceability and formation of online contracts. The general rule is that the provinces regulate internal commerce, and the federal government the interprovincial or international commerce. Thus, businesses must often deal with multiple regulatory regimes. Canadian Courts are currently using the foreseeability test to determine if Canadian, provincial or a foreign legislation applies.

It should also be noted that except for the province of Québec which independently enacted its *An Act to Establish a Legal Framework for Information Technology*, most provincial legislation governing electronic commerce and electronic transactions has been enacted and modelled on the *Uniform Electronic Commerce Act* (the UECA) which was adopted in 1999 by the Uniform Law Conference of Canada. The UECA was designed to provide provinces with consistent legislation that implemented the principles of the *United Nations Model Law on Electronic commerce*.

E-commerce entities and non-e-commerce entities are generally treated similarly, particularly with respect to provincial and federal business registration and other registration requirements. However, e-commerce entities are subject to a wide range of laws and regulations affecting various aspects of their operations, such as taxes, export control, marketing, etc., some of which will be discussed more in depth below. Key principles governing the activities of B2B e-commerce entities in Canada include the following:

- **Electronic Document Validity**: As a general principle, information or documents, such as contracts, will not be considered invalid or unenforceable if they are solely in an electronic format. Any legal requirement to provide documents in writing will be satisfied if such document is in an electronic form, as long as they remain accessible and can still be subsequently used. In addition, if there is a legal requirement to provide information to another person "in writing", the recipient must be able to retain the information and not just be shown the information on a one-time basis or otherwise. Furthermore, electronic signatures will be generally deemed as satisfying the legal requirements if, at the time an electronic signature is affixed to a document, (a) it is reliable to identify the person making it, and (b) there exists a reliable association between this electronic signature and the electronic document.
- **Consent**: Both click-wrap and web-wrap agreements are enforceable under Canadian law if the three requirements of an agreement (that is, (a) an offer, (b) an acceptance, and (c) a consideration) are met.
- **Electronic Agents**: Under provincial legislations, an electronic agent means a computer program, or any other electronic means, used to initiate an act or to respond to an electronic document or act without a review by an individual at the time of the response or act. Electronic agents are permitted to form contracts with a person. However, such transactions will be unenforceable against such person if (a) the person makes a material error in the electronic document or information used in the transaction, (b) the electronic agent does not give the person an opportunity to prevent or correct that error, (c) the person promptly notifies the other party on becoming aware of the error, and (d) where consideration is received as a result of the error, the person takes reasonable steps to return such consideration or destroy the consideration (if so instructed), and the person has not used or received any material benefit or value from the consideration.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

In addition to the above, B2C e-commerce activities are also governed by federal and provincial laws regulating a wide range of commercial activities, including those related to consumer protection.

Many provincial laws incorporate obligations and requirements drawn from the *Internet Sales Contract Harmonization Template,* which was endorsed in 2001 as a common template to cover contract formation, cancellation rights, credit card chargebacks and information provisions. Some of those obligations and requirements are the following:

- **Disclosure**: Before a consumer enters into an agreement over the Internet, the supplier shall disclose certain information to the consumer. The following information must be accessible by the consumer and the consumer must be able to retain and print it:
  - the name of the supplier and, if different, the name under which the supplier carries on its business;

- contact information that the consumer can use to contact the supplier (telephone number, address of the premises from which the supplier conducts business, fax number, email address, etc.);
- a fair and accurate description of the goods and services to be supplied to the consumer, including the technical requirements, if any, related to the use of the goods or services;
- an itemised list of the prices at which the goods and services are to be supplied to the consumer, including taxes and shipping charges;
- a description of each additional charge that applies or may apply, such as customs duties or brokerage fees, and the amount of the charge if the supplier can reasonably determine it;
- the total amount that the supplier knows would be payable by the consumer under the agreement, or, of the goods and services to be supplied during an indefinite period, the amount and frequency of periodic payments;
- the terms and methods of payment;
- the currency in which amounts are expressed, if it is not in Canadian currency;
- any other restrictions, limitations and conditions that would be imposed by the supplier; and
- various other information on the delivery or performance of the goods or services depending on the nature of such goods or services and on the provisions of the agreement.

- **Acceptance**: A supplier must provide the consumer with an express opportunity to accept or decline the agreement and to correct errors immediately before entering it.
- **Copy**: A supplier must deliver to the consumer who enters into an online agreement a copy of the agreement in writing within 15 days after the consumer enters into the agreement, which copy must contain certain prescribed information to meet this requirement.

It should also be noted that provincial consumer protection legislation also permits, in most provinces, for consumers to repudiate executory contracts for an established "cooling off" period.

That being said, as obligations vary from one province to another, legal counsel should be consulted prior to the operation of any e-commerce business in Canada.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

Canadian privacy laws have taken a comprehensive approach to regulating public and private sectors. Like e-commerce, both federal and provincial governments regulate data protection, although the legislations' core are generally very consistent from one jurisdiction to another, as they are all based on the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

As Canada's adequacy status with the European Union – which allows data to flow freely between the EU and Canada – needs to be reviewed, Canadian legislative bodies are introducing new regulations in order to adapt to the new European standard regarding the protection of personal data. In that respect, the province of Québec just introduced, on June 12, 2020, a new bill that is very similar to the GDPR in Europe. It is expected that the federal law (the *Personal Information Protection and Electronic Documents Act* (PIPEDA)) will also be amended in the near future to be consistent with the GDPR.

2.2 What privacy challenges are organisations facing when it comes to fintech, AI and digital health?

Fintech, AI and digital health organisations deal with an immense amount of sensitive data, which are used as a resource. However, the current Canadian data protection legislations have yet to fully adapt to the reality of data being a resource. Privacy laws designed to protect individuals from exploitation are framed around what were once distinct and siloed issues. While Canadian privacy laws continue to provide important protection, notably as they are technologically neutral, there remain important questions about how to ensure these frameworks have the appropriate approach to maintain the trust of citizens in an increasingly data-fuelled world. This necessity for an appropriate balance – namely between ensuring the right flexibility and agility for innovation, while maintaining user buy-in and security – is a key theme for Canadian organisations.

Moreover, with such sensitive data, fintech and health organisations need to have strong identification and authentication procedures. Unfortunately, Canada is behind in this matter, as the main identification and authentication procedures still use the Canadian social security number.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, AI and digital health?

The Government, as well as privacy, financial and other regulators, launched regulatory sandboxes to assist organisations in dealing with innovation, privacy and regulatory issues. Privacy regulators, known as privacy commissioners in Canada, are also frequently publishing and updating guidelines on the matter.

In 2019, the Government of Canada published the *Digital Charter*, and decided to move forward with an ambitious, aspirational principled approach to digital and data transformation in Canada. The principles are the foundation for a "*Made in Canada*" digital approach that will guide Canadian policy making and actions, while helping to build an innovative, people-centred and inclusive digital and data economy.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

In Canada, there are no regulations on digital security and encryption that apply specifically to e-commerce. Generally, the security warranties are provided by contract, although encryption may be essential for compliance with industry standards, more particularly for financial institutions or third-party payment processors. It should however be noted that, in most cases, an electronic transaction implies the exchange of personal information, and privacy laws provide that minimum safeguards must be implemented to protect such personal information from unauthorised reproduction and disclosure. In that regard, businesses are required to implement appropriate security safeguards to protect personal information – most importantly for B2C e-commerce – from unauthorised use, disclosure, or access.

More generally, Canada's anti-spam legislation (CASL) specifically prohibits, in the course of commercial activity, the

alteration of an electronic message so that the message is delivered to a different destination or as an addition to the one specified by the sender.

CASL also governs the installation of software in the course of commercial activities when the software provider or the target computer is located in Canada. It forbids the installation of viruses and spyware by prohibiting:

- the installation of software on another person's computer without the express consent of said owner or an authorised user of the computer;
- causing software to be installed without consent; and
- the installation of software that can communicate with other electronic devices without the consent of the owner or authorised user.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

Regarding personal health information, three provinces (Ontario, New Brunswick, and Newfoundland) have specific provincial laws providing additional protection to such data.

The Financial Consumer Agency of Canada (FCAC) monitors the financial industry's compliance with several codes of conduct. Those codes can handle various topics such as banking services to seniors, debit card services, or bank relations with small and medium-sized businesses.

More specifically, the *Principles of Consumer Protection for Electronic Commerce: A Canadian Framework* provides guiding principles to businesses in developing a consumer protection framework for electronic commerce while clarifying the responsibilities associated with the service.

Financial institutions or third-party payment processors can also decide to comply with the *Payment Card Industry Data Security* (PCI-DSS) standards.

Finally, the voluntary federal certification programme, CyberSecure Canada, can certify small and medium-sized businesses that voluntarily meet security benchmarks.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Canadian consumers have long embraced e-commerce, whose share of the overall retail market continues to grow steadily year after year. According to Canada Post's 2020 Canadian e-commerce report, "eight out of ten Canadians shopped online in 2019 and *eMarketer* estimates spending at $65 billion in 2019 – rising to almost $108 billion by 2023". As is the case in other jurisdictions, however, the most active online shoppers are concentrated in certain segments of the population and it is estimated that 60% of all online purchases in Canada are made by just 18% of online shoppers, mostly the lucrative HYPER+ segment.

According to a recent report by Absolunet, across Canada, one dollar in 10 is traded digitally in the retail space – almost on par with the US (10.7%).

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

According to J.P. Morgan, cards (both debit and credit) are the principal way to pay online in Canada, being used for 62% of all e-commerce transactions. Moreover, Canadians are more likely to pay for products outright via debit rather than taking on debt, as evidenced by the number of debit cards in circulation which is more than two times higher than the number of credit cards. Digital wallets are also increasingly popular among Canadians, accounting for 18% of the payments market.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Canadian retailers with an online presence have traditionally performed well with Canadian consumers but have also had to compete with foreign platforms as Canadians typically make a large number of cross-border transactions, especially through U.S.-based platforms. Politics, trade and exchange rates are important factors that influence shopping habits of Canadians and, as of recent years, Canadian retailers have benefited from a decline of cross-border shopping by Canadian consumers.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

E-commerce firms should be aware that more than 200 languages are spoken in Canada, with English and French being the two official languages. Most e-commerce platforms operating in Canada will be in both English and French. As J.P. Morgan points out, e-commerce platforms that offer multiple languages are likely to find success within this highly multilingual country.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

To our knowledge, the preferences of Canadians are not specifically different from those of other online consumers and, like them, they prefer clean, intuitive and frictionless web-interfaces. Furthermore, since apps are the dominant mobile commerce channel in Canada, used for 51.4% of all transactions completed on handheld devices, clear images and typefaces are essential when selling to Canada's online shoppers via mobile platforms.

It is worth noting that according to a recent report by Eagle Eye, Canadian consumers also respond very well to social selling and are more likely to visit social media platforms before making a purchase than US, Australian or UK consumers.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

There is no general process for online brand enforcement in Canada. Brand owners can instead rely on applicable laws, specifically including trademark infringement actions, unfair competition, and/or passing-off actions to prevent the illegal use of their brands.

Regarding domain names, brand owners can rely on the complaint mechanism made available under the *Uniform Domain Name Dispute Resolution Policy* (UDRP), whose goal is to resolve disputes arising from abusive registration of domain names. For .ca domain name, the CIRA's Dispute Resolution Policy (CDRP) is available.

Tools provided by private platforms can help brand owners prevent the infringing use of their brands by notifying them of any use on said platforms and providing specific tools to enforce their trademarks (e.g. Amazon Brand Registry or Alibaba Intellectual Property Protection Platform).

As an alternative, Canadian rights holders of registered trademarks can submit a request for assistance with the Canada Border Services Agency to take pre-emptive steps against counterfeit products.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

For online brand enforcement, unavailable WHOIS information or lack of any contact information for infringing parties is the most recurring restriction, making it difficult to find a way to contact or locate said infringing parties. Domain name registrars, including the Canadian Internet Registration Authority (CIRA), generally do not provide the personal information of registrants.

Regarding .ca domain names, requirements related to the eligibility of a complainant such as the Canadian Presence Requirements for Registrants (CPR) can make it difficult for foreign brand owners to use this mechanism for an abusive .ca domain name. On the other hand, the territorial nature of trademarks can also be a restriction to their enforcement when the infringing activities are occurring outside of Canada.

Private platforms may not always respond to a complaint if, for example, the infringement is ambiguous. The tools provided also have a very specific purpose and force brand owners to rely on more traditional mechanisms provided notably by trademark or competition legislation.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Since organisations that collect or process personal information have significant statutory responsibilities with respect to the collection, use and disclosure of personal information, it is essential that their relations with any third parties providing processing or hosting services are consistent with such responsibilities. Most notably:

- **Level of Protection**: Any organisation dealing with a third-party data processor must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. This obligation is normally met by entering into robust and detailed agreements and/or through other non-contractual oversight and auditing mechanisms. Such agreements should contain provisions relating, *inter alia*, to security, standards of performance, burden of compliance, breach detection and record keeping, incident response and notification.
- **Transparency**: The customers or individuals from whom an organisation collects personal information should be made aware of such organisation's practices when handling personal information, including the use of any third party-owned data centre or cloud provider. Such practices must also be consistent with the original purpose of collection for which a consent was obtained.

In addition to the privacy implications, there are also several other important elements to consider when entering into an agreement with a third party provider, such as capacity, data portability, subcontracting and assignment, indemnification and liability, effects of termination, etc. Since data is often at the heart of digital businesses, these issues need to be carefully considered.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

At the federal level, PIPEDA does not require that servers or data centres be located in Canada. However, some provincial laws contain restrictions that require some data, mostly public sector data and certain types of personal information such as health-related information, to be stored in Canada.

Even in cases where federal and provincial laws do not prevent the storage of data on servers or data centres located in other jurisdictions, it should be noted that (a) data transferred outside of Canada becomes subject to the laws of the jurisdiction where it is stored, and (b) the organisation collecting data will ultimately remain fully accountable and responsible for that data, which means that the legal implications of such transfer should always be closely considered.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

The Advance Commercial Information Definition (ACI) is an initiative of the Canada Border Services Agency which aims to provide officers with electronic information registered for all commercial cargo entering Canada. ACI has been in effect since 2004 for marine shipments and 2006 for air shipments. The ACI is inspired by its American equivalent, the Container Security Initiative (CSI).

The goal is to provide the necessary information to officers to help them identify any health, safety, or security issues with imported commercial goods prior to moving the freight in Canada, in order to efficiently highlight high-risk goods while expediting the transfer through customs of low-risk goods.

This new process helped eliminate important delays at cargo points of entry and helped achieve faster clearance of freight.

It does require some coordination prior to shipping to ensure that an acceptance is received at the necessary date. Required documents and information (i.e. commercial invoice, bill of

lading, dispatch level information, etc.) must be provided in advance so that clearances and eManifests, a special barcoded manifest, can be set up before the goods are shipped to Canada.

The final step to implement ACI is the eManifest for highway shipments and is currently under development with involvement from private and public actors.

The recent *United States-Mexico-Canada Agreement* (USMCA) also includes specific provisions related to digital trade. More particularly, it prohibits customs and other charges on digital products, but parties may continue to impose internal taxes or charges. It also commits the parties to collaborate and establish necessary and appropriate safeguards regarding cybersecurity, consumer protection, or spam prevention.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Regarding trade facilitation, the increasing amount of data collected and analysed is raising concerns for customers and businesses, notably with recent issues regarding the lack of data confidentiality and potential cybersecurity threats.

To ensure proper adoption of digital technologies, it is also necessary to provide capital investments and resources to ensure that the technology is appropriately matched with the specific needs and requirements of its users. It must also be implemented properly by transferring the necessary knowledge and skills while creating documentation and resources to ensure that it is being used efficiently.

Cooperation between the stakeholders is necessary and the states must agree on standardised rules, principles or standards, otherwise it could create disparities between digital systems, making the successful adoption of digital technologies even harder in the context of trade.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Foreign businesses and operators of online platforms that sell intangibles or services in Canada are not required to collect and remit federal and provincial sales taxes if they do not carry on business in Canada within the meaning of the *Excise Tax Act*. This would be the case, for instance, if they do not have a physical or significant presence in Canada. The province of Québec is an exception, as specific rules have been adopted.

Also, an e-commerce business can deduct from its revenues a capital cost allowance for computer software and website development costs. Digital businesses could also, in some cases, benefit from investment tax credits, including the Scientific Research and Development Investment Program. These tax incentives come in three forms: an income tax deduction; an investment tax credit (ITC); and, in certain circumstances, a refund.

Lastly, incentives may be provided at the provincial level, such as Québec's "Development of E-Business Tax Credit" which is available to a corporation that carries out its activities through an establishment in Québec.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

One of the most contentious issues is whether a digital business has a sufficient nexus to Canada to be subject to taxation. Such nexus would normally derive from corporate residency or the carrying on of a business through a permanent establishment. Authorities are now using elements such as servers and computer equipment as a link between Canada and a corporation's activities.

Another source of dispute is the characterisation of income, that is whether it qualifies as business or property income. This distinction is highly relevant, as the tax rates applicable differ between the two types of income and because property income can be subject to withholding taxes.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

In Canada, labour and employment legislation depends primarily on the sector of activity in which a business is active in. Even if most employers fall under provincial jurisdiction, certain industries are of federal jurisdiction, and as such, only federal labour laws may be applied, unless otherwise specified.

Even if the labour legislation in Canada provides for several different employment statuses (e.g. full-time, part-time, seasonal, fixed-term, indefinite term, etc.), Canadian legislation tends to put the emphasis on the employer-employee relationship rather than the status in itself. Thus, provincial acts normally apply solely to employees and exclude independent contractors or self-employed individuals.

However, the definition of "employee" is not standard across jurisdictions, hence, the protection and benefits included in the labour and employment laws will only benefit employees, in accordance with its corresponding meaning, and will not be available for independent contractors, among others.

Consequently, if a business wishes to resource work in Canada, the practical and legal considerations will depend on, first, whether its activities fall under provincial or federal jurisdiction and, second, the province in which said resource will work.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There is no specific regulation in place in Canada relating to telecommuting. Certain provinces, such as Ontario and Manitoba, have incorporated the concept of "homeworker" or "home work" within their employment standards legislation to provide individuals falling in that category with certain specific protections or obligations. Nevertheless, most provinces view telecommuting as a form of work where regular labour and employment legislation are still applicable. Despite some uncertainties surrounding its true application, provincial laws on occupational health and safety are also applicable when telecommuting.

Thus, the main regulation of telecommuting in Canada remains the internal policies instilled by employers and the agreements they concluded with their employees. Such policies will inherently depend on the employer's expectations and activities, but should focus on IT, confidentiality and privacy issues, work hours, among others.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

In general, Canada is recognised as having particularly stringent consumer protection laws with which any B2C digital business should be familiar. In addition, compliance with the French language requirements necessary to operate in the province of Québec (which represents approximately 22.5% of the Canadian population) is sometimes perceived as onerous or burdensome by some digital businesses. Lastly, digital businesses must navigate a wide array of evolving federal and provincial laws and will need to invest time and resources to understand and comply with the everchanging legal landscape.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

In addition to the fact that there are no specific registrations applicable to e-commerce, digital businesses operating in Canada have access to a fast-growing, wealthy and tech-savvy market. Since the federal and provincial governments recognise the importance of digital transformation and wish to invest in the data-driven economy, there are a number of economic initiatives that promote the development of digital businesses as well.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

In Canada, Payments Canada was established by the *Canadian Payments Act* to operate two core payment clearing and settlement systems in Canada: (a) the Large Value Transfer System (LVTS), an electronic funds transfer system that settles large-value and time-critical Canadian dollar payments; and (b) the Automated Clearing Settlement System (ACSS) for clearing of retail payments, including direct deposits, imaged paper, point-of-service and online debit transactions, pre-authorised debits, and ABM transactions. Payments Canada establishes the rules relating to such clearing and settlement systems. Digital businesses may also be required to comply with certain rules of the payment network requirements pursuant to their agreements with network participants.

Card issuers, payment processors and other participants of the credit and debit card networks must also comply with the *Code of Conduct for the Credit and Debit Card Industry in Canada*.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

The Canadian government is currently looking to implement a new retail payments oversight framework. This new framework would apply to a wide range of transactions, and a number of currently unregulated payment industry participants would be regulated as payment service providers (PSPs). As of the latest discussion paper published, this framework would mainly contain: (a) registration requirements for PSPs; (b) liability rules shielding end-users for losses as results of unauthorised transactions; and (c) various operational and safeguarding requirements for PSPs to protect end-users. Even if this retail payments oversight framework has yet to be adopted, it will considerably shake up the current framework applicable to payment service providers and should be closely monitored by digital businesses acting as such.

Acknowledgment

Special thanks to Vincent Caron, Vanessa Deschênes, Jules Gaudin, Rosalie Jetté, Élisabeth Lesage-Bigras and Julie Robert for their collaboration in the drafting of this article.

Jean-François Normand is a senior associate in the Emerging Technologies Group at ROBIC and specialises in intellectual property and information technology law. He has acquired an expertise in the high-tech industry and is involved in advising companies – from the early-stage start-ups to giant-tech companies – on issues related to e-commerce and digital marketing, data protection, privacy and cybersecurity, online brand enforcement, digital health and medical devices, digital entertainment, and open source licensing.

ROBIC LLP
2875 Laurier Boulevard
Delta 3 - suite 700
Québec G1V 2M2
Canada

Tel: +1 418 780 0962
Email: jfnormand@robic.com
URL: www.robic.ca

Founded in Montreal in 1892, ROBIC is internationally renowned and has earned a reputation for excellence in intellectual property in Canada. Our firm has offices in Montreal and Quebec City, and includes a team of over 180 support staff and highly qualified professionals specialising in intellectual property and business law.

ROBIC is one of the most prolific filers of trademarks in Canada and has earned an undeniable reputation for the quality and number of patents filed annually. Our experienced litigation lawyers, some of whom are recognised by their peers as being the best intellectual property litigators in the country, represent our clients in all courts, including the Federal Court of Canada, provincial courts in Quebec, the Supreme Court of Canada, as well as specialised administrative tribunals.

In addition to offering all intellectual property services, ROBIC has an experienced team of business lawyers whose expertise is recognised internationally.

For 125 years, ROBIC has been the benchmark for the protection and commercialisation of intellectual property rights and other intangible assets in Canada.

www.robic.ca

ROBIC 1892

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms
Workplace Pensions

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group