Stikeman Elliott

Digital Business in Canada

By Alethea Au, Vanessa Coiteux and David Elder

This article was first published on Lexology Navigator.

LEXOLOGY®
Navigator

LEXOLOGY®
Navigator

Digital Business

in Canada

Table of contents

Law stated date

- Correct as of

Contributors

Canada

Stikeman Elliott

Stikeman Elliott LLP
Alethea Au
aau@stikeman.com

Stikeman Elliott LLP
Vanessa Coiteux
vcoiteux@stikeman.com

Stikeman Elliott LLP
David Elder
delder@stikeman.com

Recent developments and future prospects

Trends and developments

Have there been any notable recent trends or developments concerning the conduct of online and digital business (both business to business and business to consumer) in your jurisdiction, including any regulatory changes or case law?

Recent rulings by the Supreme Court of Canada in Douez v Facebook (2017 SCC 33) and Google Inc v Equustek Solutions Inc (2017 SCC 34) illustrate some of the issues that digital businesses are facing as a result of the ease with which their business activities and customer relationships can cross international borders.

In Douez, the Supreme Court of Canada found a forum selection clause unenforceable against a user asserting a statutory right of action for invasion of privacy, after putting significant weight on the inequality of bargaining power between Facebook and the user. This will give digital businesses some pause as they evaluate the effectiveness and enforceability of such 'boilerplate', particularly with respect to statute-based claims. Thus, Douez might complicate the compliance strategies for such businesses.

The Supreme Court's second decision, Google Inc v Equustek Solutions Inc (2017 SCC 34), upheld a 2014 British Columbia Supreme Court injunction that effectively required Google to de-index certain IP-infringing content from its worldwide search results. The ruling confirmed the jurisdiction of Canadian courts to issue orders with extraterritorial implications where it is necessary to give effect to the injunction. However, Google subsequently obtained an order from the US District Court in California declaring the Canadian injunction unenforceable in the United States. The basis of the US decision was that enforcement of the Canadian injunction would violate a policy goal underlying the US Communications Decency Act, namely that interactive services providers such as Google should not be regarded as the publishers of the information that they make available. Armed with this ruling, Google returned to Canada to apply to have the British Columbia injunction varied or set aside. However, the British Columbia Supreme Court dismissed the application on the ground that its 2014 injunction did not actually require Google to violate US law, given that de-indexing is not illegal in that country.

These two Supreme Court rulings highlight the patchwork nature of compliance obligations facing global digital businesses whose operational and business strategies may be required to be tailored to ensure compliance with applicable regulatory regimes.

Future prospects

What are the future prospects for digital business in your jurisdiction, including any proposed or potential regulatory reforms and future technological/market developments?

Amendments to Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) come into effect in November 2018 and, among other things, will require all Canadian organisations experiencing a data breach involving personal information to:

- determine whether the breach poses a real risk of significant harm to any individual by conducting a risk assessment;
- notify affected individuals and report to the privacy commissioner of Canada as soon as feasible if the breach poses a real risk of significant harm;
- notify other organisations that may be able to mitigate the harm to affected individuals; and
- maintain a record of any data breach that the organisation becomes aware of and provide it to the commissioner on request.

If a Canadian organisation that is subject to PIPEDA experiences a data breach involving personal information and fails to abide by these rules after they are in force, it could be fined up to C$100,000. Note that the corresponding Alberta statute, the Personal Information Protection Act, has for a number of years required reporting in the event of an incident that creates a real risk of significant harm to an individual.

These amendments highlight the growing importance of and focus on threats to privacy and data security.

Looking ahead, the enhanced data protection requirements under the EU General Data Protection Regulation (GDPR) may lead to revisions to Canada's privacy laws in order to maintain its status as a country recognised as providing an adequate level of data protection, so that personal data respecting EU residents may continue to be stored and processed here without any further safeguard being necessary.

Growing concern with the effectiveness and focus of Canada's Anti-Spam Legislation (CASL) resulted in a 2017 Parliamentary Committee report recommending a number of material revisions to the law. The government's

response to the report agreed with many of the recommendations and indicated that the government would work with stakeholders to identify ways to address the concerns raised in the report. Accordingly, reform of CASL seems likely, although the timing is uncertain.

The increasingly strong public and regulatory focus on blockchain and especially cryptocurrency have resulted in the examination by securities and banking regulators of various issues relating to:

- investor protection;
- integrity of the capital markets and the banking system; and
- proceeds of crime and anti-money laundering.

As the use of this technology becomes more widespread, it is expected that the attendant risks would be further crystallised. Blockchain users may accordingly need to prepare for additional scrutiny and potential regulation.

Similarly, the increasing prevalence of Internet of Things (IoT) products and services (and the incorporation of artificial intelligence into such products and services) are expected to raise new concerns about consumer risks in the areas of privacy and data security (eg, in relation to locational data) as well as with respect to the responsibilities of IoT manufacturers and service providers.

Legal framework

Legislation

What primary and secondary legislation governs the conduct of digital business in your jurisdiction?

In Canada, the federal and provincial governments share legislative authority. Generally speaking, the federal government is responsible for laws relating to matters of a national or international importance, while provincial governments are responsible for laws relating to matters of local importance. Many areas of law that relate to trade and commerce (eg, employment law, property law, consumer protection, securities law and the law of contract) are governed predominantly by provincial legislation. Areas of federal jurisdiction that could affect digital businesses include:

- competition and misleading advertising law;
- laws relating to broadcasting;
- IP law
- anti-spam/anti-malware law; and
- private-sector privacy legislation (with the caveat described immediately below).

Privacy law straddles the constitutional division of powers between Canada and its provinces. The federal government has enacted the Personal Information Protection and Electronic Documents Act (PIPEDA). This statute generally applies to all commercial information and also contains provisions relating to e-commerce. However, any Canadian province is entitled, should its legislature so determine, to enact its own equivalent of PIPEDA, provided that the provincial legislation is "substantially similar" to PIPEDA. If a province does so, its legislation will supplant PIPEDA with respect to the collection, use or disclosure of personal information occurring within the province. To date, only Alberta, British Columbia and Quebec have enacted general provincial legislation of this type (several other provinces have done so with respect to health information privacy only).

Note also that the Canadian constitution places a number of industries under federal jurisdiction. These industries include banking, air and rail transport, broadcasting and telecoms, and a number of others. In these industries, federal laws in areas such as labour and employment and privacy apply in situations that would otherwise be governed by equivalent provincial laws.

Regulatory authorities

Which authorities regulate the conduct of digital business and what is the extent of their powers?

There are no regulatory authorities specifically tasked with regulating digital business in Canada. Instead, Canadian digital businesses are regulated by the same agencies that regulate brick-and-mortar businesses. The authorities that digital businesses might expect to engage with include the privacy commissioner (of Canada or of a province), the Competition Bureau (notably with respect to advertising), the Canadian Radio-television and Telecommunications Commission (notably with respect to anti-spam laws), provincial securities regulators and the Canadian Intellectual Property Office. Such regulators have powers similar to those in most other countries,

generally including the issuance of recommendations and the creation of rules with respect to which investigations may then be conducted, which may (depending on the regulator and the circumstances) lead to undertakings or other corrective measures, fines, injunctions or in some cases prosecutions. There is no distinction between digital businesses and other businesses in respect of the exercise of any of these powers.

Government policy and regulatory approach

How would you describe the government's policy and regulatory approach to digital business?

Digital businesses in Canada are treated similarly to other businesses. Digital businesses are regulated by the same agencies and subject to the same laws as brick-and-mortar businesses, and Canada's e-commerce legislation imposes a media-neutral approach to commercial information. All electronic communications and documents are considered functionally equivalent to those made on paper.

Establishing digital businesses

Requirements

What regulatory and procedural requirements govern the establishment of digital businesses in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

There are no government requirements specific to digital business establishment in Canada. Like all businesses, digital businesses must register their business name, comply with regulations and obtain licences and permits relating to the goods that they sell. If they wish to have the benefits of incorporation, they must incorporate under the federal Canada Business Corporations Act or under one of the similar acts that is in force in each province. While large corporations with nationwide operations often choose to incorporate federally, there is no necessity to do so as provincially incorporated corporations can operate extra-provincially with the appropriate registrations.

Electronic contracts and signatures

Electronic contract availability

Are electronic contracts legally valid in your jurisdiction? If so, what rules and restrictions govern their formation (including any mandatory or prohibited provisions and contract formats)?

Canadian e-commerce legislation supplements traditional contract law to enable the enforceability of electronic contracts in Canada. Because the law of contract is a provincial responsibility in Canada, the key legislation in this area is provincial. In all provinces except Quebec, the e-commerce statute is based on the principles enunciated in the UN Model Law on Electronic Commerce, adopted in 1996 (Quebec's e-commerce law implements many of the same principles but does not follow the UN Model Law directly). Canada takes a functional equivalency approach to e-commerce, so electronic contracts are legally valid where there is offer and acceptance. Both web-wrap and click-wrap agreements have been recognised by the Canadian courts, but only where the offer and acceptance requirements are met. For example, in Rudder v Microsoft (1999, 2 CPR (4th) 474), the court held that clicking on an 'I agree' icon served as valid acceptance of an offer. But in Aspencer1.com Inc v Paysystems Corporation (JQ no 1573, JE 2005-601), a Quebec judge held that an organisation could not modify the terms of a contract by posting them on its website, on the grounds that there was no proof of real acceptance by the user.

Are there any limitations or restrictions on transactions that can be concluded through electronic contracts?

No limitations or restrictions specifically apply to commercial electronic transactions in Canada.

Data retention

Do any data retention requirements apply to electronic contracts?

There are no data retention requirements specific to electronic contracts in Canada. Instead, electronic contracts are viewed as functionally equivalent to paper contracts and are therefore subject to the same data retention requirements as those contracts done in writing. For example, the Canada Revenue Agency requires all tax

documents to be retained for at least six years. Provincial electronic transaction legislation provides that electronic records are equivalent to paper originals where the electronic documents have integrity (ie, are complete and unaltered) and where they are retainable.

Remedies

Are any special remedies available for the breach of electronic contracts?

Provincial consumer protection legislation specifically addresses internet agreements and allows customers to cancel agreements if certain criteria are not met. Some examples of where an internet agreement may be cancelled by the consumer under provincial legislation include:

- where certain information is not disclosed;
- where the consumer was not given a meaningful opportunity to accept, decline or correct errors in the agreement prior to acceptance;
- where the consumer has not accessed the relevant information; and
- where the consumer is unable to retain or print the information.

Electronic signatures

Are electronic signatures legally valid in your jurisdiction? If so, what rules and restrictions govern their use?

Electronic signatures are legally valid in Canada. Provincial e-commerce acts provide that the legal requirement of a signature is satisfied by a signature produced electronically. However, exceptions apply in a variety of cases, including wills, powers of attorney, negotiable instruments, affidavits, certain business incorporation and corporate finance documents, and documents in which IP rights are granted.

Best practices relating to e-signatures in Canada include:

- giving proper notice that e-signatures will be used;
- ensuring that the method of collecting the e-signatures complies with privacy requirements; and
- maintaining accurate records on the consent to use, accept and the delivery of e-signatures.

Electronic payments

Electronic payment systems

Are there any rules, restrictions or other relevant considerations regarding the use of electronic payment systems in your jurisdiction?

Businesses that use electronic payment systems in Canada will need to consider the impact of privacy and consumer protection laws. Provincial privacy legislation applies to electronic payment systems that retain consumer data. There are also industry standards and guidelines, such as the Payment Card Industry Data Security Standard (PCIDSS) rules, which aim to protect consumer information during the electronic payment process. The PCIDSS rules are not mandatory or enforceable, but they are often considered as a best practice. Some of these rules include ensuring that:

- only necessary consumer data is made available to acceptors during a transaction;
- the acquirer or acceptor cannot access a consumer's account balance at any time;
- a firewall configuration is maintained to protect cardholder data;
- the transmission of cardholder data across open, public networks is encrypted; and
- access to physical cardholder data is restricted.

Financial institutions that offer mobile wallet services in Canada agree to abide by the mobile wallet provisions of the Code of Conduct for the Credit and Debit Card Industry in Canada. These provisions require financial institutions offering mobile wallet services to allow consumers to:

- select which payment source they want to use for each transaction;
- easily change electronic payment settings; and

- clearly see each payment source on the app.

Requirements relating to mobile wallets, like the above, are enforced by the Financial Consumer Agency of Canada.

Virtual currencies

Are there any rules or restrictions on the use of virtual currencies (eg, Bitcoin)?

No rules or restrictions apply exclusively to virtual currencies in Canada yet, but securities legislation, as well as anti-money laundering (AML) and terrorist financing legislation, can apply to virtual currency offerings and transactions.

The Canadian Securities Administrators (CSA), the umbrella organisation of Canada's provincial securities commissions, provides guidance to Canadians on the applicability of securities laws to virtual currencies. In a notice released in 2017, the CSA mentioned that cryptocurrency offerings will be regulated as securities offerings and specified that whether securities law applies to a given cryptocurrency transaction will depend on substance, not form. For example, an offering of tokens granting access to a video game is less likely to raise securities law issues than an offering of tokens the value of which depends on the future success of a business.

AML and terrorist financing legislation also affects businesses that deal in virtual currencies. The Proceeds of Crime (Money Laundering) and Terrorist Financing Act has been amended to require businesses dealing in virtual currencies to register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Canada's federal financial transactions analysis unit. However, the regulatory framework required to implement this type of registration is not yet in place. Draft regulations were released on 9 June 2018 and appear unlikely to be in effect (in their finalised form) before late 2019. When fully in force, the new regime will require registration with FINTRAC and the establishment of an AML compliance programme, led by a chief AML officer.

Data protection and cybersecurity

Collection, use and storage

What rules, restrictions and procedures govern the collection, use and storage of personal data in the course of digital business in your jurisdiction?

Personal data collection, use and storage in Canada are governed by a combination of federal and provincial privacy legislation. The federal Personal Information Protection and Electronic Documents Act (PIPEDA) sets standards that are also followed in corresponding provincial legislation where it exists. Key principles emphasised by PIPEDA and its provincial equivalents include:

- accountability;
- consent;
- limiting use;
- safeguards;
- individual access;
- identifying purpose;
- limiting collection;
- accuracy;
- openness; and
- challenging compliance.

Consumers with privacy concerns may complain to the privacy commissioner of Canada (or the provincial counterpart) if an organisation is not following its privacy obligations under PIPEDA or a provincial privacy act. The privacy commissioner can then investigate the matter and order organisations to correct their practices where appropriate. The commissioner may also take unresolved matters to the Federal Court of Canada and seek a court order to rectify the situation.

International data transfers

What rules and restrictions apply to the cross-border transfer of personal data collected in the course of digital business?

In Canada, privacy laws applicable to the private sector do not prohibit cross-border transfer of personal data, but they do impose requirements on organisations that outsource information processing. PIPEDA and similar provincial acts require organisations that transfer data outside Canada to explain clearly to consumers that their

information may be processed in a foreign country when their personal information is collected.

For digital businesses that may serve enterprise and institutional clients, it should be noted that a number of sector-specific laws, such as federal laws respecting banking and insurance, require that certain records be retained in Canada. In addition, the provinces of British Columbia and Nova Scotia have enacted laws that generally prohibit the storage or processing outside Canada of personal information held or under the control of government agencies and public institutions (eg, universities and hospitals), subject to narrow exceptions that vary between those provinces.

Consumer rights

What rights are afforded to consumers in relation to their personal data?

PIPEDA gives consumers a right of informed consent when their data is collected: organisations that collect personal information from consumers must specify the reason that they are collecting the data and, having done so, must not use the information for any other reason. Data collection must also be limited to what is necessary for the stated purpose and the organisations that collect data must keep it confidential and be transparent with respect to their data management practices.

Consumers with privacy concerns about an organisation can complain to the appropriate privacy commissioner and request an investigation into the organisation's practices. If a deficiency is found, the organisation may be advised or subjected to a court order to change its practices or an award of damages by the court.

Cookies

How is the use of cookies regulated?

Canada has no legislative requirements that specifically target cookies. Two avenues by which cookies could potentially be regulated are Canada's anti-spam legislation (CASL) and policies of the privacy commissioner:

- While generally requiring prior express consent for the installation of computer programs on another's computer system, CASL explicitly excludes the installation of cookies from this requirement, deeming consent to the installation of cookies in all circumstances in which the person's conduct indicates such consent. Examples in which consent would not generally be implied in this way include situations in which a website attempts to override the consumer's disabling of cookies or Javascript in their browser.
- In 2015, the privacy commissioner of Canada's Policy Position on Online Behavioural Advertising generally affirmed a principle of opt-out consent, provided that organisations maintain adequate transparency about their practices (including through "online banners, layered approaches, and interactive tools") and that information collected excludes, to the extent possible, sensitive information (particularly health and medical information). This approach does not apply to so-called 'zombie cookies', 'supercookies', third-party cookies that are disguised as first-party cookies and other techniques that lie outside the consumer's control.

Data breach

What rules and standards govern digital operators' response to data breaches? Are they subject to any notification requirements in the event of a data breach? What precautionary measures should be taken to avoid data breaches?

In June 2015, the Digital Privacy Act amended PIPEDA to include data breach requirements. These new provisions come into force in November 2018 and will require all Canadian organisations experiencing a data breach to:

- determine whether the breach poses a real risk of significant harm to any individual by conducting a risk assessment;
- notify affected individuals and report to the privacy commissioner of Canada as soon as feasible if the breach poses a real risk of significant harm;
- notify other organisations that may be able to mitigate the harm to affected individuals; and
- maintain a record of any data breach that the organisation becomes aware of and provide it to the commissioner on request.

If a Canadian organisation that is subject to PIPEDA experiences a data breach relating to personal information and fails to abide by these rules after they are in force, it could be fined up to C$100,000. Note that the corresponding Alberta statute, the Personal Information Protection Act, has for a number of years required reporting in the event of an incident that creates a real risk of significant harm to an individual.

To avoid a data breach, organisations should consider, among other things:

- adopting a cybersecurity policy;
- using encryption;
- training employees about data breach risks and best practices relating to passwords, encryption keys and software updates;
- collecting, storing and transferring only data that is actually required; and
- organising a breach response team, developing an incident response plan and regularly testing security measures, including by means of simulated breaches.

Additional breach avoidance recommendations are available from the federal and provincial privacy commissioners' offices.

Cybersecurity

What cybersecurity regulations and/or standards apply to the conduct of digital business?

A number of federal and provincial statutes regulate cybercrime in Canada.

Canada's Criminal Code, which is federal legislation that applies in all provinces, criminally prohibits non-consensual interception of online communication and imposes prison sentences of up to five years for offenders. CASL, the federal anti-spam law, prohibits non-consensual software installation on computer systems, while PIPEDA (and the corresponding laws in some provinces) requires Canadian organisations to take preventative cybercrime measures, including ensuring that:

- security safeguards are in place to protect personal information (eg, locking filing cabinets and using encryption); and
- personal information is protected against theft, copying, disclosure, modification or unauthorised access.

The Canadian Securities Administrators also provide guidance to Canadian businesses on how to prevent cybercrime. Recommendations include securing client information, training staff to follow best practices relating to data protection, creating incident response plans and social media and cybersecurity policies, and regularly testing security measures for efficacy.

Is cybersecurity insurance available and commonly purchased?

Cybersecurity insurance is available in Canada. Although cybersecurity policies are becoming increasingly common, a 2018 FICO survey found that only 40% of Canadian firms had cybersecurity insurance that covered all likely risks, with 22% still having no coverage at all. Cybersecurity insurance coverage is highly customisable and may vary substantially from one provider to another.

Encryption

Are there regulations or restrictions on the use of encryption?

No legislation or regulation restricts the use of encryption in Canada. In 2016, the federal government held a national security consultation that addressed questions relating to encryption. At the consultation, participants debated whether encryption should be restricted in Canada for security reasons. No restrictions have been implemented, but the encryption debate in Canada is ongoing.

Government interception/retention

What rules and procedures govern the authorities' interception of communications and access to consumer data?

Canadian law enforcement and national security agencies may obtain judicial authorisation to intercept communications, preserve evidence and perform searches. Currently, there is no general power to require that any individual or company provide law enforcement with the means to access decrypted devices, although court orders that compel disclosure may be obtained in specific circumstances. A number of laws compel businesses to provide a range of business records, including customer data, to various sectoral regulators on demand, in the course of an investigation.

Advertising and marketing

Regulation

What rules govern digital advertising and marketing in your jurisdiction?

Canada has general competition laws and specific anti-spam laws that apply to digital advertising.

As for competition law, the federal Competition Act applies to all online representations. Representations may relate to online or offline sales. In addition, if an advertisement originates outside Canada but may influence the Canadian public, the Competition Act may apply.

Canada's anti-spam legislation (CASL) applies to the use of "commercial electronic messages", including advertisements. Businesses may not send commercial electronic messages without the explicit consent of the recipient. Commercial electronic messages must also be in a prescribed form, including information such as sender identification and contract details and a no cost, easy unsubscribe mechanism. There are some exceptions to these new rules. For example, existing business relationships may not have to adhere to the stricter requirements outlined above.

Are there any specific regulations governing the use of targeted advertising?

Canada does not have specific regulations on the use of targeted advertising, but privacy laws may apply.

The federal Office of the Privacy Commissioner (OPC) has released a policy position (Policy Position on Online Behavioural Advertising) on how the federal Personal Information Protection and Electronic Documents Act (PIPEDA) would apply to targeted advertising. For example, under PIPEDA, organisations must receive meaningful consent for the collection, use and disclosure of personal information. According to the OPC, this would include personal information used for targeted advertising.

Restrictions

Are there any restrictions or limitations on goods and services that can be advertised, marketed and sold online?

Goods and services sold online are generally subject to the same restrictions that apply to the same sales for brick-and-mortar establishments. For example, vendors must comply with consumer protection legislation in each province and territory.

Spam messages

What rules and restrictions govern the sending of spam messages?

CASL imposes strict limitations on the use of "commercial electronic messages". Businesses may not send commercial electronic messages without the explicit consent of the recipient. Commercial electronic messages must also be in a prescribed form, including information such as sender identification and contract details and a no cost, easy unsubscribe mechanism. There are some exceptions to these new rules. For example, existing business relationships may not have to adhere to the stricter requirements outlined above.

Digital content and IP issues

Required notices

Are websites and any other digital content required to display certain legal notices or other information in your jurisdiction?

Federal privacy laws, provincial consumer protection laws and federal anti-spam laws impose informational requirements on digital content in certain circumstances.

The federal Personal Information Protection and Electronic Documents Act (PIPEDA) requires organisations to provide their privacy policy to individuals for the collection, use and disclosure of personal information.

The consumer protection legislation of a number of provinces, including Ontario, British Columbia, Nova Scotia and Quebec, requires certain information to be disclosed in online consumer contracts. The information required to be disclosed in internet agreements under Ontario's legislation includes:

- online retailer names;
- contact information;
- a fair and accurate description of the goods and services;
- an itemised list of prices;
- a description of each additional charge that applies or may apply;
- the total amount payable by the consumer;
- the terms and methods of payment;
- the details of delivery or performance (including date, place and manner of execution); and
- any specific rights or obligations with respect to cancellations, returns, exchanges and refunds.

CASL requires commercial electronic messages to include information such as sender identification, contact details and a simplified unsubscribe mechanism. CASL also generally requires prior express consent for the installation of a computer program on another's computer system, which would include mobile apps. Federal guidance indicates that self-installed programs are not covered by the law, provided that the functionality of the program is clearly disclosed to the user prior to installation. Enhanced notification is required for a range of functionality commonly associated with malware, such as collecting personal information stored on the user's device and interfering with the user's control of the device.

Liability for content

What rules govern liability for online or other digital content that is defamatory or infringes another party's IP rights?

In the common law jurisdictions of Canada, the common law of defamation generally covers online content. To establish defamation, the relevant content must be defamatory, relate to the person claiming defamation and be published at least once to a third party. In Quebec, Article 1457 of the Civil Code of Quebec, which sets out the general rules of conduct applicable to all persons, is the basis of the law of defamation. The common law provinces also have defamation legislation, known either as the Defamation Act or the Libel and Slander Act.

In Canada, the federal Copyright Act governs the law of copyright, regardless of registration. The Parliament of Canada amended the federal Copyright Act in 2012, enacting provisions such as the "Notice and Notice Regime" requiring internet service providers (ISPs) to pass on notice of a copyright infringement to an infringing user. The Copyright Act describes infringing and non-infringing conduct in detail.

Although trademarks do not need to be registered in Canada, the federal Trade-marks Act generally covers trademark law in Canada, including offences relating to the improper use of trademarks.

How can liability be excluded or limited?

Liability can generally be limited or excluded in three ways. First, the requirements for the relevant offence should be considered. For example, a defamatory statement must objectively lower the respect for the plaintiff in the community. Second, there may be exceptions to the offences outlined above even if an offence is otherwise committed. For example, fair dealing allows users of copyright material to reproduce it for the purpose of research and education, under certain conditions. Third, trademarks can be licensed in Canada under the Trade-marks Act, allowing the use of a trademark without committing an offence.

Which parties can be held liable for defamatory or infringing content? Can contingent liability be extended to internet service providers (ISPs)?

The extent to which third parties such as ISPs can be held liable for defamation likely depends on whether they have engaged in re-publishing the defamatory content. For example, in one Canadian case, Crookes v Newton (2011 SCC 47), the Supreme Court of Canada held that simple hyperlinks to defamatory content will not constitute defamation.

The Copyright Act does not attribute liability to third-party conduits such as ISPs as long as they are acting as a neutral intermediary. However, these conduits may be liable and/or have obligations imposed on them if a party holding a copyright provides them with a notice of infringement. For example, under the Notice and Notice regime set out in the Copyright Act, an ISP would have to forward the notice to the infringing user and retain records to identify the infringing party.

There is no similar legislation for trademarks. Nonetheless, ISPs may be subject to court orders for injunctive relief, including removal of infringing content.

Content takedowns

What rules and procedures govern content takedowns? Can ISPs remove defamatory or infringing content without permission?

The common law of injunctions governs content takedowns. A party will therefore have to obtain a court order to take down content infringing on its rights. There is no legislation requiring ISPs to take down content once they have received notice that the content infringes copyright, trademark rights or other IP rights. In a closely related development, the Supreme Court of Canada in Google Inc v Equustek Solutions Inc (2017 SCC 34) upheld an injunction issued by a lower court that effectively required Google to de-index certain IP-infringing content from its worldwide search results.

Domain names

What rules, restrictions and procedures govern the licensing of domain names?

The Canadian Internet Registration Authority (CIRA) manages the '.ca' country code through accredited registrars. CIRA has established several rules for the registration of '.ca' domain names, including the Canadian presence requirements, which restrict registration to individuals and organisations that are sufficiently connected to Canada (eg, being a citizen or permanent resident, in the case of an individual). Corporations incorporated in Canada are also eligible, as are Canadian trusts, partnerships and unincorporated associations, provided that they meet certain tests. Of particular interest to non-Canadian entities is the provision permitting any holder of a trademark that is registered in Canada under the Trade-marks Act to apply to register the "exact word component" of the mark as a '.ca' domain.

It should be noted that there is no requirement to use the '.ca' domain names in Canada, and many businesses use '.com' or other top-level domains (TLDs) in place of or in addition to '.ca'. Registration of a '.com' domain name is effected in the same way as in other countries and does not involve CIRA.

How are domain name disputes resolved in your jurisdiction?

CIRA manages the rules and procedures for resolving '.ca' domain name disputes under the Canadian Dispute Resolution Policy. A registrant must submit to a proceeding under the CIRA Dispute Resolution Rules if a complainant has asserted the following:

- the registrant's '.ca' domain name is confusingly similar to a mark in which the complainant had rights prior to the date of registration of the domain name and continues to have such rights;
- the registrant has no legitimate interest in the domain name as described; and
- the registrant has registered the domain name in bad faith.

In a recent situation that illustrates how these principles work, the global messaging platform Whatsapp was able to secure the 'whatsapp.ca' domain name from a cybersquatter who was found to have registered the name without a legitimate interest and in bad faith. The fact that Whatsapp, a US company, had registered its trademark in Canada was sufficient to satisfy the Canadian presence requirements referred to in the previous question. The matter was resolved by the British Columbia International Commercial Arbitration Centre, one of two designated resolution service providers for '.ca' disputes, in addition to Resolution Canada Inc.

Disputes involving '.com' and other generic TLDs are handled under generally applicable processes established by the Internet Corporation for Assigned Names and Numbers.

IP protection measures

What special measures and safeguards should rights holders consider in protecting their online/digital content?

Generally, the best way to protect rights is through registration.

As for IP rights, registration will usually provide broader protection even if statutory protections apply to unregistered rights holders. For example, any party infringing on a registered copyright will be deemed to have knowledge of the copyright. Similarly, trademark registration will automatically give the holder nationwide protection whereas an unregistered trademark must have sufficient reputation in a geographic area to receive protection, creating ambiguities for online and digital content.

As for domain names, registration can protect the domain name for one to 10 years and can include common variations of the domain name as well a French version of the name (or English version of a French name).

Tax issues

Online sales

How are online sales taxed?

Pursuant to the federal Excise Tax Act, businesses must charge and collect the 5% goods and services tax (GST) from customers on taxable goods and services supplied in Canada in the course of a business carried on in Canada. All provinces except Alberta also levy a comparable tax at the provincial level:

- In Quebec and the Western provinces (other than Alberta), the provincial tax is distinct from GST.
- In Ontario and the Atlantic provinces, the provincial tax has been harmonised with GST to form a single harmonised sales tax (HST) that is collected by the federal government, with the provincial part being remitted by it to its respective provincial counterparts. For example, in Ontario, the federal (5%) and provincial (8%) taxes are combined into a single HST of 13%.

Note that the GST, HST and Quebec's provincial tax are value added taxes (VATs), while the provincial taxes of Manitoba, Saskatchewan and British Columbia are sales taxes that do not generally apply to services and often exempt certain categories of good from their application (these exemptions vary from province to province).

Whether online sales will be taxed depends on where the vendor carries on business and where the customer is located. Whether a person is carrying on business in Canada will depend on a consideration of all relevant facts. However, commonly considered factors in the context of the application of GST and HST are listed below:

- the place where agents or employees of the non-resident are located;
- the place of delivery;
- the place of payment;
- the place where purchases are made or assets are acquired;
- the place from which transactions are solicited;
- the location of assets or an inventory of goods;
- the place where business contracts are made;
- the location of a bank account;
- the place where the non-resident's name and business are listed in a directory;
- the location of a branch or office;
- the place where the service is performed; and
- the place of manufacture or production.

Similar factors are considered for provincial sales tax.

Online sales into Canada are generally subject to the payment of amounts equivalent to the taxes that would have been payable had the sales occurred within Canada, although a remission (essentially a waiver) is granted for most shipments valued at less than C$20.

Other taxes

What other tax liabilities arise in respect of the conduct of digital business in your jurisdiction?

In Canada, income tax is imposed by both the federal and provincial governments, but not by cities or other municipalities. In all provinces other than Quebec, both federal and provincial income taxes are paid by means of a single return.

Income tax applies to digital businesses in the same way as other businesses. That said, the geographically indeterminate nature of many digital businesses can make it more difficult to determine the jurisdiction in which income tax should be paid. While it is impossible to review all of the relevant principles here, the most fundamental rules are as follows:

- Canadian residents are taxed on their worldwide income. Depending on the relevant entity and facts, residency may depend on tests set out in the federal Income Tax Act or in the common law.
- Non-residents are taxed on income from a business carried on in Canada, employment income earned in Canada and on taxable capital gains from the disposition of "taxable Canadian property". However, tax treaties may modify the taxation of non-residents.

For federal income tax, a person is generally considered to carry on business in Canada if the person concludes contracts in Canada, or if the operations from which the profits arise are located in Canada. Additionally, the Income

Tax Act may deem a person to be carrying on business in Canada if the person solicits orders or offers anything for sale in Canada through an agent or servant. Advertising is generally not sufficient to meet this test.

Similar rules apply to residents and non-residents for provincial income tax.

Jurisdiction, governing law and dispute resolution

Jurisdiction and governing law

How do the courts determine jurisdiction and governing law in relation to online/digital transactions and disputes?

Without a forum selection clause, Canadian courts will usually assert jurisdiction if a real and substantial connection exists between the forum and either the proceeding or the defendant. Historically, the Canadian courts have used one of the three tests below to determine jurisdiction in relation to online and digital transactions and disputes:

- Passive versus active test – Canadian courts examine the level of interaction available to individuals in their jurisdiction. If interaction with the website is possible, the court will generally find a sufficient connection to its jurisdiction. This test has become obsolete with the growth of interactive websites and with the growing sophistication of content-only websites.
- Purposeful direction test – if an internet presence is purposefully directed towards individuals in a jurisdiction, this will form a real and substantial connection.
- Foreseeability test – if the parties would have reasonably foreseen that they would become answerable to a foreign court, then this may form a real and substantial connection.

Of the tests above, the courts have most frequently used the foreseeability test in recent cases.

Some forum selection clauses may not be enforceable after the recent Supreme Court of Canada decision in Douez v Facebook (2017 SCC 33). In Douez, the court found a forum selection clause unenforceable after putting significant weight on the inequality of bargaining power between Facebook and the user.

For choice of law, different rules apply for procedure, contracts and general civil liability. For procedural matters, a Canadian court will use the law of its jurisdiction. For contracts, the law with the most significant connection to the contract will govern unless the law is chosen in the contract. In the case of a tort, the choice of law will depend on where the tort was committed, with a similar principle applying with respect to the corresponding Quebec civil law concept of 'extra-contractual liability'.

Courts

Are there any specialist courts in your jurisdiction which deal with online/digital issues and disputes?

Canada does not have courts specifically for online or digital issues. However, the Canadian Internet Registration Authority requires that '.ca' domain name disputes be resolved by Resolution Canada Inc or the British Columbia International Commercial Arbitration Centre.

Alternative dispute resolution

What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

Canada has three common forms of ADR that can be used for online or digital disputes:

- negotiated settlements;
- mediated settlements; and
- arbitration.

Negotiated settlements are the most popular form of ADR, with the majority of disputes settling. Mediation has also become popular partly because courts in some jurisdictions may require mediation before parties can go to trial. Although mediation is recommended by the Federal Court of Canada, which has jurisdiction over IP disputes, it is not yet mandatory. Businesses in Canada also frequently choose arbitration to resolve disputes because of its flexibility and confidentiality.

Online versions of the above have also become more popular (eg, British Columbia's Civil Resolution Tribunal and

the eBay Resolution Centre).

Law stated date

Correct as of

Please state the date of which the law stated here is accurate.

20 August 2018

About Stikeman Elliott

Stikeman Elliott is a global leader in Canadian business law and the first call for businesses working in and with Canada. Our offices are located in Montréal, Toronto, Ottawa, Calgary, Vancouver, New York, London and Sydney. We provide clients with the highest quality counsel, strategic advice, and workable solutions. The firm has an exceptional track record in major U.S. and international locations on multijurisdictional matters and ranks as a top firm in our primary practice areas including mergers and acquisitions, securities, business litigation, banking and finance, competition and foreign investment, tax, restructuring, energy, mining, real estate, project development, employment and labour, and pensions.

For more information about Stikeman Elliott, please visit our website at www.stikeman.com.

Contact us

Alethea Au
aau@stikeman.com

Vanessa Coiteux
vcoiteux@stikeman.com

David Elder
delder@stikeman.com

Follow us

SE

Subscribe to updates on a variety of legal topics from Stikeman Elliott's Knowledge Hub at stikeman.com/kh

Stikeman Elliott LLP

Montréal Toronto Ottawa Calgary Vancouver New York London Sydney

Stikeman Elliott