

GETTING THE DEAL THROUGH

e-Commerce

in 31 jurisdictions worldwide

Contributing editor: Robert Bond

2009



**Published by
Getting the Deal Through
in association with:**

ABBC – Azevedo Neves, Benjamim Mendes, Bessa Monteiro, Carvalho & Associados, Sociedade de Advogados RL

Abdulai, Taiwo & Co

Altius

Barretto Ferreira, Kujawski, Brancher e Gonçalves – Sociedade de Advogados (BKBG)

Dimitrov, Petrov & Co

Foyen Advokatfirma AB

Froiep Renggli

García Magliona y Cia Ltda

Gatt Frendo Tufigno Advocates

George Charalambides & Co

Hankyul Law Firm

Heydary Hamilton PC

J Sagar Associates

Joyce A Tan & Partners

JUDr. Tomas Borec Law Firm

Jun He Law Offices

Karniol Malecki i Wspólnicy Sp k

Latournerie Wolfrom & Associés

LG@vocats

Loebl & Loebl

Lovells

Martí & Associats

Michalsons Attorneys

Minter Ellison Lawyers

Portolano Colella Cavallo Studio Legale

Preslmayr Rechtsanwaelte OG

Schjødt

Speechly Bircham LLP

SSW Schneider Schiffer Weihermüller

Yabuki Law Offices

Canada

Javad Heydary, Eb Reinbergs, Nasser Ashgriz, Tanya Walker, Victor Opara and Daisy Yu

Heydary Hamilton PC

General

- 1** How can the government's attitude and approach to internet issues best be described?

Canada is a leading jurisdiction when it comes to assisting with the establishment of a global standards process for the regulation of e-commerce. The Canadian federal government is also a world leader in the adoption, use, and development of e-business, and has developed various strategies to encourage the growth of e-commerce. For example, the Canadian government is committed to a 'technology-neutral' approach to electronic commerce taxation which avoids internet-specific taxes. It has also implemented policies in the areas of privacy protection, online security and appropriate internet content. These policies are designed to integrate e-business into the Canadian economy by increasing the level of trust and confidence that businesses and consumers have in the digital environment.

Legislation

- 2** What legislation governs business on the internet?

The following is a list of federal legislation which regulates business being conducted on the internet:

- the Competition Act, RSC 1985, c.C-34;
- the Copyright Act, RSC 1985, c.C-42;
- the Criminal Code, RSC 1985, c.C-46;
- the Investment Canada Act, RSC 1985, c.28;
- the Personal Information Protection and Electronic Documents Act, SC 1999-2000, c.5;
- the Telecommunications Act, SC 1993, c.38; and
- the Trademarks Act, RSC 1985, c.T-13.

With respect to provincial legislation, all the provinces and territories except for the Northwest Territories have enacted legislation governing electronic commerce. Furthermore, every province but Quebec has modelled its e-commerce legislation on the Uniform Law Conference of Canada's Uniform Electronic Commerce Act (the Uniform Act). The Uniform Act is designed to implement the principles of the United Nations Model Law on Electronic Commerce, adopted by the United Nations General Assembly in November of 1996. The legislation is designed to be media neutral, recognising electronic communications, documents, contracts, and signatures as equivalent to their counterparts.

A few provinces, such as Ontario, Saskatchewan, Manitoba, and Nova Scotia, have also adopted consumer protection legislation, part of which governs online sales contracts entered into by consumers.

Regulatory bodies

- 3** Which regulatory bodies are responsible for the regulation of e-commerce and internet access tariffs and charges?

E-commerce is generally governed by the Electronic Commerce Branch of Industry Canada (Industry Canada). Organisations operating under the umbrella of Industry Canada, including the Canadian Intellectual Property Office, Canada's Office of Consumer Affairs, and Spectrum, Management and Telecommunications Sector, also provide for the regulation of e-commerce in Canada.

The Canadian federal government has also established a Public Key Infrastructure (PKI) initiative, which is working to establish a legal framework that will give Canadians security and confidence to use the internet when conducting business, and to facilitate e-commerce nationally and internationally in a secure environment.

Neither the Canadian government, nor the provincial governments, impose any specific internet access tariffs and charges. The Canadian government is committed to a 'technology-neutral' approach to taxation.

Jurisdiction

- 4** What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions (or contentions) in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

The development of the law of jurisdiction in the context of virtual communications is still in its infancy. Traditional law with respect to contract and tort applies to online transactions. However, there still remains a jurisdictional challenge with respect to the application of law to contract and tort matters.

The mere act of downloading a product is not enough to settle the question of jurisdiction. Recently, the courts in Canada have evaluated the nexus between the forum in which proceedings are filed, the parties involved and the substance of the lawsuit.

The real and substantial connection test has been applied to determine the nexus of the location of the servers, employees, offices and bank accounts. In order to determine whether presence has been established in Canada, or that the business is carried on in Canada, the courts have paid attention to factors including whether the defendant adhered to Canadian laws, paid Canadian taxes, advertised, marketed, or had other specific content aimed at the Canadian market.

In obiter, the courts have discussed the targeting test that is currently applied in the United States, but have not applied it. The targeting test presupposes that the online conduct in question is targeted towards the locale being asked to assert jurisdiction over a website because the conduct is accessible there and there is evidence available to demonstrate that the site actively targets an audience within the

jurisdiction. There is also the need to evaluate the language and content of the site, terms and conditions posted on the site and awareness that the site's content may be accessed in a different jurisdiction.

The court and the legislature have yet to establish case law or legislation with respect to online defamation. With respect to traditional defamation actions, the plaintiff must demonstrate that the alleged defamatory posting was accessed, downloaded and read by someone in the jurisdiction where there is damage to the plaintiff's reputation. The court will also pay attention to whether the author of the libelous comment knew or should have known that the target of their posting or article resides in a particular place, the rationale being that a person's reputation will suffer most where their reputation is greatest.

Contracting on the internet

- 5** Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?

Parties are generally free to enter into electronic contracts. The general rules of contract formation apply. A contract is formed on the internet when acceptance of an offer is communicated by the offeree to the offeror, and consent is given.

One way to form a contract over the internet is through the use of 'click wrap' agreements, whereby a party enters into a contract when they click the 'I agree' or 'I accept' button, signalling acceptance of the vendor's terms and conditions. Click wrap contracts are generally enforceable in Canada. An Ontario court held that electronic contracts are not materially different from a multi-page document requiring a party to turn the pages of the contracts. As long as the fundamental rules of contract formation are in place, click wrap contracts are enforceable. However, one should note that in this particular case, in reaching a decision that the click wrap contract was enforceable, the judge took into account the fact that the plaintiffs were law students and thus had a legal background. In a case where the plaintiff was not as technologically and legally adept, the outcome may be different.

- 6** Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

All provinces and territories except for the Northwest Territories have adopted specific legislation to govern e-commerce. Such legislation addresses issues relating to electronic documents equivalency, digital signatures, and electronics record retention. Generally, such legislation does not distinguish between business-to-consumer and business-to-business contracts. However, many provinces have enacted consumer protection legislation which only governs business-to-consumer contracts. For example, the Ontario Consumer Protection Act, 2002, SO 2002, c.30, was implemented to protect consumers who conduct online transactions. Vendors and suppliers must meet various requirements before the internet agreements entered into with consumers are deemed valid.

While there is provincial legislation which distinguishes between business-to-consumer and business-to-business contracts, the general principles of contract law in Canada do not make such distinctions.

- 7** How does the law recognise or define digital or e-signatures?

In Canada, although electronic transactions are provincially regulated, some federal laws have defined and recognised electronic signatures. For example, the Personal Information Protection and

Electronic Documents Act (PIPEDA) defines 'electronic signature' as 'a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document'. Notwithstanding, each Canadian province or territory has its own domestic laws that recognise or define digital or electronic signatures for purposes of commercial contracts.

In Ontario, for example, the Electronic Commerce Act regulates electronic transactions. The Act defines 'electronic' to include things 'created, recorded, transmitted or stored in digital form or in other intangible form by electronic, magnetic or optical means or by any other means that has capabilities for creation, recording, transmission or storage similar to those means'. The Act goes further to define 'electronic signature' to mean 'electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document.' Like other provincial legislation governing electronic commerce, Ontario's Act provides that where there is a legal requirement that a document be signed or endorsed, that requirement is satisfied by an electronic signature, so long as the electronic signature is reliable for the purpose of identifying the person signing the document, it is reliable to associate the electronic signature with the relevant electronic document, and any additional requirements that may be prescribed for specific documents are satisfied.

In Quebec, the Quebec Information Technology Act regulates electronic transactions. The Quebec Act recognises the validity of electronic signatures. The Quebec Act is similar to Ontario's Act in terms of reliability of electronic signatures, and will recognise electronic signatures that are appended to electronic documents whose integrity have not been compromised and there is an ongoing link between the signature and the document from the time of signing up to the relevant time that the evidence is required.

- 8** Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

There are various federal statutes which govern the issue of data retention with respect to the creation, maintenance, and retention of electronic records that affects the conduct of business over the internet. For example, Canadian privacy legislation (PIPEDA) has addressed the issue of data retention in the private sector. PIPEDA requires, among other things, consent to be obtained before retaining information. Businesses must also identify the purpose for the collection of information, and must provide adequate security for the retention of information.

Aside from PIPEDA, the following are examples of Canada's federal legislation which address the issue of electronic records retention:

- Canada Business Corporations Act, RSC 1985, c.C-44; and
- Customs Act, RSC 1985, c.1.

Each of the provinces have enacted legislation which has supplemented PIPEDA by developing retention policies with respect to electronic contracts. For example, in the Province of Ontario, the Electronic Commerce Act sets out the legal requirements that must be met with respect to the retention of electronic documents. A document that was originally created, sent or received electronically satisfies the legal requirements for retention if: (i) the electronic document was retained in the format in which it was created, sent or received, or in a format that accurately represents the information contained in the document that was originally created, sent or received; (ii) if the retained information contained in the electronic document will be accessible so as to be usable for subsequent reference; and (iii) if the information that identifies the origin and destination, and the

date and time of when the electronic document was sent or received is also retained.

In Quebec, the purpose of the Quebec Information Technology Act is to provide for the 'legal security of documentary communications', regardless of the medium used. With respect to the retention of electronic records, the act stipulates that during the period a document is to be retained, the integrity of the electronic document must be maintained, and equipment must be available to ensure the document is 'accessible, intelligible, and usable' for the purposes for which the document was intended.

Security

9 What measures must be taken by companies or ISPs to guarantee the security of internet transactions?

In Canada, there are various sources of legal obligations with respect to the security of internet transactions. Notwithstanding, Canadian law does not generally stipulate the particular kind of technology, standards or yardsticks that must be adhered to in any given situation. Rather, where there is a security requirement for internet transactions, Canadian law has always favoured a broad and open approach to those security requirements with the aim of giving electronic transactions a wider scope to improve their security measures on an ongoing basis.

The use of the internet by companies or ISPs for exchange of commercial documents and business transactions is increasing. Transactions made in open networks like the internet increasingly involve dealings with unknown parties who do not have any pre-existing relationship with the company or ISP. As such, trust becomes an essential element to internet transactions. For companies or ISPs to rely on internet transactions, reliability and securely authenticated communications are needed. Measures to achieve these ideals include ensuring that there are means of identifying the parties conducting the transaction and associating those parties with the contents of the e-communications. Authentication of internet transactions is therefore a necessary pill for the prevention of unauthorised access and fraud, among other commercial hazards of internet transactions. Other forms of authentication include passwords, access codes, internet firewalls, biometrics and encryption, among others.

Notwithstanding, companies or ISPs should note that it is not advisable to conclude all commercial transactions over the internet. Therefore, to guarantee security of internet transactions, companies or ISPs should ensure that their e-communications satisfy certain statutory requirements. One major requirement is that for some documents, the use of e-signatures and the use of e-documents, as well as the exchange of e-communications should comply with legal requirements of form. Most Canadian provinces have enacted the Statute of Frauds, which requires writing and signature in order for a document to be authentic. For example, in Ontario, the Electronic Commerce Act does not apply to the following transactions:

- wills and codicils;
- trusts created by wills or codicils;
- powers of attorney relating to an individual's financial affairs or personal care;
- documents, including agreements of purchase and sale, that create or transfer interests in land and require registration to be effective against third parties;
- negotiable instruments; and
- documents that are prescribed or belong to a prescribed class.

The Canadian Copyright Act, Patent Act and Trademark Act all need to be in writing, signed by the owner of the right to be authentic. It would therefore be prudent for companies and ISPs to ensure that certain transactions, although commenced over the internet,

are concluded in person, since this will assist in the process of authentication.

10 As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

At present, although various certification authority companies have commenced operations in Canada, and various international certification authorities offer their services to companies operating in Canada, there is no statutory framework or government agency in Canada that is seized with the function of accreditation and regulation of certification authorities. Generally, there is no obligation to disclose private keys to any governmental authority. Notwithstanding, there are circumstances that may warrant the government of Canada or its provinces and territories to obtain or demand the disclosure of private keys pursuant to a court order, provided the court has the requisite jurisdiction to make such order. The Criminal Code of Canada, the Canadian Security Intelligence Act, and other acts of Parliament such as the Competition Act are a few of the federal statutes that authorise the issuance of such an order, so long as the requisite conditions for the order are met. These acts provide law enforcement and national security agencies with powers to intercept communications and search and seize information in a manner consistent with the rights and freedoms guaranteed in the Canadian Constitution and the Charter of Rights and Freedoms, particularly the right to be secure against unreasonable search and seizure. Moreover, in civil proceedings, an order for the disclosure of a private key might be made if a court of competent jurisdiction is convinced that such an order is necessary for the interest of justice. Apart from these exceptions, various provincial statutes and the common law protect encrypted communications and private keys as confidential materials.

In 2002, the government of Canada, through the Department of Justice, set up a Lawful Access Consultation forum that collated comments from the law enforcement, industry, privacy and information commissioners, civil society groups as well as the general public. The summary of the submissions made to the Consultation was released on 23 April 2003. This is part of the efforts of Canada to establish a legislative and regulatory framework for lawful access to encrypted communications. The government blueprint released pursuant to this consultation proposes various amendments to the Criminal Code and other federal statutes so as to authorise law enforcement and national security agencies to intercept wirelines, wireless or internet communications, as well as search and seize electronic information.

Domain names

11 What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

Prior to late 2000, the University of British Columbia, located in Vancouver, had the responsibility of overseeing the management and operation of the Canadian '.ca' domain name registry. In late 2000, there was a shift in the regulatory process and this function was transferred to the Canadian Internet Registration Authority (CIRA). A basic condition for registration of a .ca domain name in Canada is a 'Canadian presence requirement' (CPR). This requirement was introduced into the CIRA registration regime after its public consultation. The aim of the requirement is to ensure that the .ca domain space is developed as a key public resource for the social and economic development of all Canadians. CIRA's Canadian presence requirement means that registrants must fit into at least one of 18 listed categories:

- Canadian citizens;
- permanent residents of Canada;
- legal representatives of Canadian citizens or permanent residents;
- corporations incorporated under Canadian federal, provincial or territorial law;
- trusts established in Canada;
- partnerships registered in Canada;
- Canadian unincorporated associations;
- Canadian trade unions;
- Canadian political parties;
- Canadian educational institutions;
- Canadian libraries, archives or museums;
- Canadian hospitals;
- Her Majesty the Queen and her successors;
- Indian bands recognised by the Indian Act of Canada;
- aboriginal peoples indigenous to Canada;
- government or government entities in Canada;
- trademarks registered in Canada by a non-Canadian owner; and
- official marks registered in Canada.

Applicants for a .ca domain name who fail to meet the Canadian presence requirement during the registration process will have their applications terminated and any associated domain names cancelled. The documents required by CIRA or CIRA certified registrars to confirm that a registrant meets the Canadian presence requirement include, but not limited to:

- Canadian government-issued photo identification (eg, driver's licence);
- articles of incorporation;
- registration number of official mark;
- registration number of trademark;
- trademark documentation; and
- partnership agreement.

It is possible to register a .ca domain name in Canada without being a resident of Canada. Under CIRA's Canadian presence requirement, there are two listed categories that permit non-Canadian residents to register a .ca domain name. The first is a non-resident of Canada who owns a trademark that is registered in Canada. It is immaterial how the owner obtained ownership. However, the permission to register a .ca domain is limited to an application consisting of or including the exact word component of the registered trademark. The second class of non-residents of Canada who can register a .ca domain name are those who have registered their badge, crest, emblem, official mark or any other mark in Canada through the registrar of trademarks. However, this permission to register a .ca domain name is limited to an application consisting of or including the exact word or component of such badge, crest, emblem, official mark or any other mark in respect of which application was made to the registrar of trademarks.

12 Do domain names confer any additional rights (for instance in relation to trademarks or passing off) beyond the rights that naturally vest in the domain name?

In Canada, the registration of a .ca domain name does not confer any additional rights on the registrant beyond the rights that naturally vest in the domain name under the Canadian Internet Registration Authority (CIRA) regulatory framework. Unlike some courts in the United States that have recognised property rights in domain names, Canadian courts and adjudicators have not taken such a radical approach in their resolution of domain name disputes. On the

contrary, decisions of the Domain Name Dispute Resolution Policy (CDRP), the dispute resolution branch of CIRA, appear to indicate that a domain name registrant could be stripped of the right to use the domain name if the registrant infringes the common law rights of another person to an unregistered trademark or the statutory rights of a registered trademark owner. The factors that the CDRP considers in arriving at its decisions include the following: (i) that the use of the trade name (or trademark) commenced prior to the registrant's registration of the .ca domain name and that such use has created a reputation capable of causing the trade name (or trademark) to be identified with the complainant's business; (ii) that the registered domain name resembles the complainant's trade name (or trademark) in sound, appearance or ideas such that it is confusingly similar to the trade name and is likely to be mistaken for the trade name; (iii) that the registrant and the complainant are in the same or similar line of business; and (iv) that the registrant registered the domain name in bad faith with the aim of diverting the complainant's internet users to registrant's business internet site. In the same vein, where a registrant can prove that the domain name is used for the purpose of distinguishing its wares or services from those of others, the registrant may seek registration of the domain name as a trademark with the Canadian Intellectual Property Office (CIPO) under the acquired distinctiveness exception under the Canadian Trademarks Act.

13 Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

Ownership of a trademark will assist a complainant in challenging a 'pirate' registrant who has obtained a .ca domain name so long as the trademark is registered in Canada. In Canada, the Federal Court has jurisdiction over matters of trademark disputes. Ownership of a trademark duly registered in Canada accords the trademark owner a statutory right to use that trademark across Canada without any interference by others. However, resolution of trademark disputes through the Federal Court could be expensive as it involves a full judicial process. In an attempt to provide a forum in which bad faith registration of .ca domain names are dealt with relatively quickly and inexpensively, the Canadian Internet Registration Authority (CIRA) implemented a Dispute Resolution Policy (CDRP) in 2002. The CDRP charts the CIRA's procedures and rules for addressing .ca domain name disputes. Under the CDRP framework, eligible complainants must, at the time of submitting a complaint, satisfy the following criteria: CIRA's Canadian presence requirement in respect of the domain name that is the subject of the proceeding unless the complaint relates to a trademark that is registered in Canada and the complainant is the owner of the trademark; and if CIRA transfers the disputed .ca domain name to the complainant or a nominee of the complainant, at the time of transfer, the complainant, or nominee will satisfy the Canadian presence requirement in respect of the domain name that is the subject of the proceeding. Accordingly, ownership of a trademark registered in Canada will not only assist the trademark owner to challenge a pirate registrant of a .ca domain name, but will also assist the trademark owner in taking over the transfer of the .ca domain name at the end of the CDRP resolution process if the decision is in favour of the trademark owner since ownership of the trademark is one of the listed categories of the Canadian presence requirement. In order to submit a complaint under the CDRP framework, a complainant must satisfy three conditions: that the registrant's .ca domain name is confusingly similar to a trademark in which the complainant has rights prior to the date of registration of the domain name and continues to have such rights; that the registrant has no legitimate interest in the domain name; and that the registrant has registered the domain

name in bad faith. The procedural framework categorically permits registrants and complainants to submit their disputes, at any time during the CDRP resolution process, to a judicial or administrative proceeding, arbitration, mediation or any other procedure they may deem necessary.

Advertising

14 What rules govern advertising on the internet?

Advertising in Canada is regulated by statute and the common law. Relevant legislation includes:

- the Competition Act, RSC 1985, c.C-34;
- the Consumer Packaging and Labelling Act, RSC 1985, c.C-38;
- the Textile Labelling Act, RSC 1985, c.T-10;
- the Precious Metals Marking Act, RSC 1985, c.P-19; and
- the Food and Drugs Act, RSC 1985, c.F-27.

Various other provincial consumer protection and tobacco acts in addition to numerous statutes governing business and trade practices also have a bearing in this area. The Charter of French Language in Quebec also provides restrictions on the style and content of advertisements, many of which are designed to preserve the prominence of the French language in the province.

The Competition Act provides a dual criminal and civil adjudicative regime whereby the commissioner of competition may pursue an action in either realm when confronted with representations that are materially false, fraudulent or misleading. The legal principles of recklessness and wilful blindness will also apply to third-party websites that publish misleading information.

Various bills continue to be introduced to the House of Commons with an objective towards amending the Competition Act. Bill C-19, which was introduced in the House of Commons and received first reading on 2 November 2004, would, among other things, allow the Competition Tribunal to impose an administrative monetary penalty (AMP) if it finds that a person or company abused its dominant position or has engaged in deceptive marketing. Bill C-41 was introduced in the House of Commons and received first reading on 7 December 2006. The bill amends the Competition Act by providing a new power to the Competition Tribunal to order a telecommunications service provider to pay an AMP if it abuses its dominant position. The amount imposed may be up to C\$15 million. Neither bill has received royal assent.

15 Are there any products or services that may not be advertised or types of content that are not permitted on the internet?

Numerous provincial and federal laws restrict the advertising of sexually explicit material, tobacco products, offensive material and firearms. Additionally, an advertisement will contravene the law if it contains a representation that is either false or misleading.

Financial services

16 Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and if so by whom and how?

The financial services industry in Canada is regulated both federally and provincially. Banks, federally incorporated insurance companies, trust and loan companies and credit unions are regulated by the federal government through the Office of the Superintendent of Financial Institutions (OSFI). Provincially incorporated insurance companies, trust and loan companies and credit unions are regulated by their respective provincial governments through similar organisations.

OSFI was created to contribute to public confidence in the Canadian financial system. The organisation's role is to:

- supervise institutions and pension plans to determine whether they are in sound financial condition and meeting minimum plan funding requirements respectively, and are complying with their governing law and supervisory requirements;
- advance, implement and administer a regulatory objective and framework that promotes the adoption of policies and procedures designed to control and manage risk;
- promptly advise institutions and plans in the event there are material deficiencies and take or require management, boards or plan administrators to take necessary corrective measures expeditiously; and
- monitor and evaluate system-wide or sectoral issues that may impact institutions negatively.

Financial services products in Canada are governed by provincial securities legislation and securities regulatory authorities. Very often, provincial securities commissions work in tandem to enact national policies. Certain national policies have been implemented in response to the adoption of the internet by the financial services industry. National Policy 47-201 regulates the trading of securities using the internet and other electronic means and National Policy 11-201 regulates the electronic delivery of documents.

Defamation

17 Are ISPs liable for content displayed on their sites?

Generally speaking, ISPs cannot be held liable for violations of Canadian copyright law committed by subscribers. Canada has yet to develop legislation specific to internet intermediaries. The role of an ISP is to provide the means for telecommunication of published materials and an ISP is shielded from liability under 2.4(1)(b) of the Copyright Act, which states that participants in a communication that only provide the means necessary for telecommunications are deemed not to be communicators.

In practice, however, the courts evaluate the role of the ISP to determine whether an intermediary such as an ISP acts as a conduit for communication or the role of the ISP is mixed. There are two types of ISP: pure ISP, where only access is provided, and mixed ISP, where the ISP is heavily involved in the dissemination of material. The court evaluates the nature of the ISP and determines whether there were circumstances that should have led the ISP to suspect that its users might have made libelous statements.

The ISP is entitled to presume that its facilities will be used in accordance with the law. ISPs do not grant licenses or permission to subscribers that permit infringement. Just as telephone companies are not responsible for the conduct of their subscribers or the content of the phone calls on their systems, ISPs contend that they should not be held responsible for the conduct of their users or content accessed on their networks.

With respect to obscene material and child pornography, an ISP and its directors might be charged under the Criminal Code for any public web page that it hosts that contains obscene material. In this circumstance, ISPs may have a duty to periodically review all pages for the acceptability of their contents and require all users to sign an advance written agreement which covers the limits of material which will be hosted by an ISP.

If an ISP is warned of a defamatory message, the court must examine the ISP's conduct in response to the complaint.

18 Can an ISP shut down a web page containing defamatory material without court authorisation?

All ISPs in Canada ensure that they have the contractual right to shut down a website they are hosting if it contains defamatory material by ensuring that their user agreement contains a provision to that effect.

Moreover, it should be noted that there is no duty or obligation on an ISP in Canada to voluntarily disclose the identity of an IP address or provide information in an alleged defamation claim. Claimants that wish to retrieve the identity of the website owner have followed the trend of naming the owner of the ISP address as John Doe, then requesting that the court order provision of the necessary contact information, as they would be entitled to it in an examination for discovery.

Intellectual property

19 Can a website owner link to third-party websites without permission?

A website owner can link to third-party websites without permission. A universal resource locator (URL) is merely a descriptive pointer to a website's address. There is no original content for an URL to fall under the purview of Canadian copyright law.

20 Can a website owner use third-party content on its website without permission from the third-party content provider?

No, a website owner cannot use third-party content on its website without permission. Canadian copyright law protects all original literary, dramatic, musical, or artistic works. The exclusive rights of the copyright owner includes the right to produce or reproduce the work; publish the work; and authorising others to produce or reproduce the work on the copyright owner's behalf. If the third-party content is original, then publishing this content on a web page without the copyright owner's permission would be considered to be both an unauthorised reproduction of the work and an unauthorised communication of the work to the public, which is a violation of Canada's copyright laws.

21 Can a website owner exploit the software used for a website by licensing the software to third parties?

Website software may be used by third-party users directly from a website under an application service provider services agreement, or through transferring the software via a licence provided by the website provider. Each situation is governed by the law of contracts. A website provider must first ensure that it has the right to transfer or license the software. In either situation, the contract will contain standard terms and conditions addressing the rights granted, term, territory and other restrictions on use.

22 Are any liabilities incurred by links to third-party websites?

Liabilities will be incurred if the creation of a hyperlink infringes copyright in Canada. This will largely be dependent on whether the link can be shown to reproduce an original work or constitute a communication to the public without the authorisation, express or implied, of the copyright owner.

Canadian law does not recognise copyright in a title of a book, play, or music. Universal resource locator (URL) addresses are considered to be analogous to titles. Accordingly, there is no copyright in a URL address itself, and the reproduction of another web page's URL will not likely be viewed as an infringement of copyright, and no liabilities will be incurred by links to third-party websites.

Data protection and privacy

23 What legislation defines 'personal data' within the jurisdiction?

The Privacy Act was enacted to further protect the privacy of individuals with respect to personal information held by a governmental institution. Section 3 defines 'personal information' to mean information about an identifiable individual that is recorded in any form, including:

- information relating to race, national or ethnic origin, colour, religion, age, or marital status of the individual;
- information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- any identifying number, symbol or other particular assigned to the individual, such as a social insurance number; and
- the address, fingerprints or blood type of the individual.

The Personal Information Protection and Electronic Documents Act (PIPEDA) also defines 'personal information'. PIPEDA defines personal information broadly. 'Personal information' is simply information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organisation.

There is various legislation, such as the Access to Information Act, RSC 1985, c.A-1, which refers to the term 'personal information'. However, such legislation generally uses the definition as established in the Privacy Act.

24 Does a website owner have to register with any controlling body to process personal data? May a website provider sell personal data about website users to third parties?

A website owner does not have to register with any controlling body to process personal data. However, a website owner that processes personal data must comply with the requirements set out in the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA applies to every organisation that collects, uses, or discloses personal information in the course of commercial activities, and it establishes rules to govern the collection, use and disclosure of personal information in a manner that balances the right of privacy of individuals with respect to their personal information and the need of organisations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. Thus, while website owners have a right to process personal data, PIPEDA will generally allow personal data to be collected or used only with the knowledge and consent of the individual.

The same rule applies with respect to the sale of personal data of website users. A website provider will be entitled to sell personal data about website users to third parties only if consent is obtained from the website users.

25 If a website owner is intending to profile its customer base to target advertising on its website, is this regulated in your jurisdiction?

Profiling customers for the purpose of advertising is not specifically regulated in Canada. The website provider must ensure that the profiling methods used do not violate privacy laws. Semi-anonymous profiling systems that do not identify individuals, such as 'cookies', do not constitute the collection of personal information and will not amount to a violation as long as the information collected cannot be combined with other databases to identify the target individual.

26 If an internet company's server is located outside the jurisdiction, are any legal problems created when transferring and processing personal data?

The collection of personal information within Canada is subject to privacy legislation. The location of the collector's server is irrelevant. A company is responsible for all personal information collected by it and requires the knowledge and consent of the individual before disclosing such information to third parties. Once consent is obtained, the company must still ensure that third parties do not use or disclose the information for purposes other than those for which consent was given.

Taxation

27 Is the sale of online products (for example, software downloaded directly from a website) subject to taxation?

In Canada, the tax laws that apply to traditional commerce also apply to electronic commerce. Generally, sales of online products by and/or to residents of Canada are subject to taxation. However, for non-residents who do not have a place of business in Canada, sales of online products are not considered to be carrying on business in Canada, and therefore, do not subject the seller to Canadian income tax on profits from the sales. However, there are sales tax liabilities. The seller of online products in Canada may be responsible for:

- goods and services tax (GST), which is currently 5 per cent;
- provincial sales tax (PST), which ranges between 5 per cent to 10 per cent in different provinces;
- harmonised sales tax (HST), which is currently 13 per cent; and
- retail sales tax (RST).

Provinces in Canada have different tax requirements on the sale of online products. These are as follows:

- HST for Nova Scotia, New Brunswick, Newfoundland/Labrador;
- GST for British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, Prince Edward Island, Northwest Territories, Nunavut, Yukon; and
- PST/RST for orders shipped to customers.

However, Alberta, the Northwest Territories, Nunavut and Yukon do not collect PST or RST. Thus, customers residing in those jurisdictions are not subjected to such taxes.

28 What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

The determining factor for the taxation in various jurisdictions is the place in which the business is carried on. Since the internet provides an opportunity for companies to conduct business in a jurisdiction while outside the jurisdiction, identification of the location of transaction can be difficult.

The issue of placing servers outside of the home jurisdiction was recently addressed by the Canadian courts. The Canada Revenue Agency (CRA) won the right to examine files of those Canadians who generate at least US\$1,000 a month in billings from their online sales. In order for the CRA to affect its rights, the Federal Court of Canada required eBay Canada, the online auctioneer, to provide tax officials with a wide range of information on the eBay sellers. eBay had argued that the servers that housed the required information were located outside Canada (California) and therefore was not within Canadian jurisdiction. However, the court noted that the information is readily and instantaneously available to those within the group of eBay

Update and trends

The most significant pending legislative event effecting e-commerce in Canada is reforms to the Copyright Act.

entities in a variety of places and it is irrelevant where the servers or the electronically stored information is located. This ruling allows Canada to tax sellers of online products who conduct business in Canada, even though their servers are located outside of Canada.

29 When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

Sales of online products by sellers outside of Canada are generally subject to taxation, and even non-residents are asked to register, collect and remit goods and services taxes (GST). Non-residents may be asked to post security at the time of registration. The GST is administered by the Canada Revenue Agency (CRA).

In addition, sellers of online products who are non-residents of the province in which the products are being sold are generally required to collect and remit provincial sales taxes (PST). Specifically, in British Columbia, Saskatchewan and Manitoba, if the out-of-province seller of online products meets all of the following four conditions, he or she must register to pay PST: (i) solicit sales in the province through advertising, mail, internet, or other means; (ii) accept purchase orders, including e-mail order, originating in the province; (iii) sell goods to a resident of the province; and (iv) cause the goods to be delivered to a location in the province, of which delivery can be done physically or electronically.

In Ontario, sales of online products by sellers outside of the province to customers located in Ontario are subject to retail sales tax (RST) if the sellers have a business presence in Ontario. If the sellers do not have a presence in Ontario, the province still recommends collection and remittance of RST, but it is not required.

In Quebec, the provincial government requires that out-of-province sellers register, collect and remit sales tax. Lastly, Prince Edward Island does not have any legislation on out-of-province seller registration. Instead, the province's Revenue Act puts the onus for remitting the Revenue Tax on the purchasers.

Small business owners do not have to charge and remit GST. However, they may be liable for harmonised sales taxes (HST). It is recommended that those who sell goods and services from one province to another voluntarily register for GST, since they are required to pay HST, and consequently GST as part of HST, to HST provinces, which are Nova Scotia, New Brunswick, and Newfoundland and Labrador.

30 If an offshore company is used to supply goods over the internet, how will returns (goods returned in exchange for a refund) be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

Return of goods and services have different tax consequences in different provinces of Canada due to the difference in their respective tax laws. Generally, a customer who has paid sales taxes, including GST and other provincial taxes, is entitled to a refund of the taxes paid upon returning the goods.

Gambling

- 31** Is it permissible to operate an online betting or gaming business from the jurisdiction?

Under the Criminal Code, the provincial government is authorised to license gaming activities in Canada. Otherwise, gaming continues to be illegal in Canada. It is a Criminal Code offence to operate a commercial gaming enterprise.

The courts will consider the intent and effect of an internet enterprise where Canadian residents are spending money on or profiting from commercial gaming in order to determine whether sufficient 'connecting facts exist to justify extending criminal jurisdiction over this activity'.

Operators of internet sites physically located in Canada that offer unlicensed internet gambling may run afoul of the offence of keeping a gaming or betting house under section 201 of the Criminal Code because it enables persons to place bets or to play games for gain. Section 201 cannot be applied to sites located outside of Canada.

- 32** Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

It is currently illegal to advertise internet gaming websites in Ontario if the operation of the site contravenes the Criminal Code. In addition, there is a private member bill in Ontario that would amend legislation to add a prohibition on advertising on internet gaming business website addresses unless the gaming business is registered in Ontario. The act has received royal assent.

However, Canadian case law concerning the legality of online gaming sites is less than clear. Residents are permitted to use online casinos and betting websites if the resident has a credit card and is of legal age, although it is difficult to monitor whether or not under-aged residents are gambling.

Outsourcing

- 33** What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

There are a number of regulatory issues that must be considered during an outsourcing transaction. The Competition Act, the Investment Canada Act, bulk sales laws, securities laws, and the OSFI Outsourcing Guideline should be consulted for the details of rules and regulations on this issue. For instance, transactions amounting to more

than \$50 million must meet all requirements outlined in Canada's Competition Act. Other issues, such as employment and regulation on highly regulated industries must also be addressed prior to an outsourcing arrangement.

In addition, a number of tax issues may arise in an outsourcing transaction. For instance, a non-resident of Canada is required to obtain a certificate pursuant to section 116 of the Income Tax Act when disposing of taxable Canadian property upon termination or expiration of an outsourcing arrangement. And, unless there is an applicable treaty exemption, the non-resident will be required to pay Canadian income taxes on any gain resulting from the disposition.

Commodity taxes may also be applicable upon an outsourcing arrangement. GST, PST and HST (see questions 27 and 29) may be payable on the transfer of taxable goods and services involved in the outsourcing transaction. In the event that the assets that are subject to the transfer constitute all or substantially all of the assets of a business, the parties may execute an election so that GST does not apply. In addition, if the outsourcing arrangement involves scientific research and development, the Canadian federal government and some of provinces will offer certain tax credits. Therefore, the outsourcing arrangement may consider utilisation and allocation of such tax credits.

- 34** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, do the rules apply to all employees within the jurisdiction?

Each province and territory in Canada has enacted its own employment law and has prescribed its own standards for employment. However, employees that work in certain federally regulated industries, such as banking, telecommunications, and air transportation are governed by federal employment laws. One of the important employment regulations in Canada is the requirement for notice of termination. Employees are entitled to 'reasonable' notice of termination or pay in lieu of notice. In the case of termination due to outsourcing, substantial notice of termination, pay in lieu of notice or severance payments might be required (or both). Therefore, the parties should determine who will bear such costs. In addition, the outsourcing arrangement might raise complex pension law issues that will have to be resolved.

HEYDARY HAMILTON^{PC}

Lawyers, Trade-mark & Patent Agents

Javad Heydary

jheydary@heydary.com

439 University Avenue
Suite 1200
Toronto, Ontario, M5G 1Y8
Canada

Tel: +416 972 9001
Fax: +416 972 9940
www.heydary.com

Online publishing

35 When would a website provider be liable for mistakes in information that it provides online? Can it avoid that liability?

Website providers are responsible for the information they post online. Mistakes in information posted are subject to statutory, civil and contractual liability depending upon the nature of the information and the damages suffered by the complainant. Liability may be avoided by complying with statutory regulations, the performance of thorough due diligence reviews, and providing for contractual limitations of liability with suppliers of content and end users. Contractual limitations may be inserted into the terms and conditions of use for the website.

36 If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

Four principle methods are used to stop third-party users from using or reproducing data provided on a website: (i) terms and conditions limiting use and reproduction may be provided for in a contractual agreement between the website provider and the end user; (ii) the Copyright Act of Canada provides the owner of an original work with the exclusive right to use and reproduce said work; (iii) unauthorised users may face potential civil and criminal liabilities; and (iv) software programmes and advances in technology may be applied to the website to prohibit users from having the ability to cut, paste or use information provided.