2001

The Internet in Light of Traditional Public and Private International Law Principles and Rules Applied in Canada

Jean-Gabriel Castel

Osgoode Hall Law School of York University, castel@fake.osgoode.yorku.ca

Follow this and additional works at: http://digitalcommons.osgoode.yorku.ca/scholarly_works

Part of the Communications Law Commons, Internet Law Commons, and the Jurisdiction Commons

This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 License.

Recommended Citation

The Internet in Light of Traditional Public and Private International Law Principles and Rules Applied in Canada

J.-G. CASTEL

INTRODUCTION

In general, the jurisdiction of a state to prescribe, to adjudicate, and to enforce is related to physical location. Yet, physical location is foreign to the Internet, which can be defined as the electronic medium of worldwide computer networks within which

---

According to para. 401 of the Restatement of the Law Third, Foreign Relations Law of the United States, (1987), vol. 1, at 232 [hereinafter Restatement of the Law Third], jurisdiction to prescribe, to adjudicate and to enforce is defined as follows:

§401. Categories of Jurisdiction

Under international law, a State is subject to limitations on

(a) jurisdiction to prescribe, i.e., to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things, whether by legislation, by executive act or order, by administrative rule or regulation, or by determination of a court;

(b) jurisdiction to adjudicate, i.e., to subject persons or things to the process of its courts or administrative tribunals, whether in civil or in criminal proceedings, whether or not the State is a party to the proceedings;

(c) jurisdiction to enforce, i.e., to induce or compel compliance or to punish non-compliance with its laws or regulations, whether through the courts or by use of executive, administrative, police, or other nonjudicial action.

With respect to jurisdiction, the Restatement of the Law Third contains rules that are accepted by Canada. See also Restatement of the Law Third, paras. 402 and 404.

---

1 According to para. 401 of the Restatement of the Law Third, Foreign Relations Law of the United States, (1987), vol. 1, at 232 [hereinafter Restatement of the Law Third], jurisdiction to prescribe, to adjudicate and to enforce is defined as follows:

2 Also called cyberspace. Another description of this word is all media used to transmit information, either digitally or electronically.
online communication takes place. As a network of computer networks interconnected by means of telecommunications facilities using common protocols and standards to allow for the exchange of information between each connected computer, the Internet is indifferent to the physical location of the computers between which such information is routed. There is no centralized storage location, control point, or communication channel for the Internet. Although each of the networks that make up the Internet is owned by a public or private organization, no single person or entity owns the Internet. It is capable of rapidly transmitting information without direct involvement or control by the end-user. Communications can be re-routed if one or more individual links are damaged or unavailable in order to deliver the information to its destination. Physical location and national boundaries are not obstacles to the ability of an individual to access websites and transact business or disseminate information anywhere in the world. Since the Internet has no territorially based national boundaries, users uploading or downloading data from unknown physical locations have no knowledge of the existence of such boundaries. This absence of physical location calls into question the applicability of the traditional public and private international law principles and rules that are based primarily on territoriality, in order to delineate the jurisdiction of states and their courts over the Internet and its users. As Judge Preska of the United States District Court in American Library Association v. Pataki explains, Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location; while


4 The Worldwide Web, which is a component of the Internet, is a collection of documents containing text, visual images, and audio clips, that is accessible from every Internet site in the world. It is used as a method of organizing information distributed across the Internet. The information on a web page resides on a computer until it is accessed by a reader. Hyperlinks are highlighted text or images that, when selected by a user, permit the user to view another related web document.
computers on the network do have "addresses," they are logical addresses on the network rather than geographic addresses in real space. The majority of Internet addresses contain no geographic clues and, even when an Internet address provides such a clue, it may be misleading.\(^5\)

Access to the Internet can enable users to evade national regulations in order to process information in violation of privacy laws, to avoid consumer protection laws, to obtain professional advice from persons not properly licensed, to hire persons in contravention of labour laws, to infringe intellectual property rights with impunity, to publish defamatory material, to access pornography, to disseminate hate literature, to circumvent gaming laws, to avoid security regulations, and so on.

Before examining the public and private international law principles and rules relevant to the Internet, it is necessary to understand who are the principal actors involved who may be prosecuted or sued in Canadian courts. First, there is the user who accesses and views or uses electronic content found on the Internet. For instance, the user visiting a website or posting information thereon may be a gambler, a purchaser of goods or services, a seeker of information, a seller of goods or services, or a gaming merchant.\(^6\) Second, there is the Internet service provider (ISP), which connects the user's computer to another computer. It allows the user, who is not directly connected to the Internet, to access it and to log onto a website and access its web contents, which is hosted by that particular computer (for instance, Bell Sympatico acts as an ISP). In other words, an ISP acts as an intermediary and gatekeeper by allowing computers connected through the network to communicate, transmit, and receive information worldwide. Individuals and businesses purchase access from an ISP, which is generally privately owned. The connection is usually made through a dial-up telephone service, although faster access is available by using a connection through integrated service digital network lines or a

---


\(^6\) Individuals can establish a link with the Internet by using a computer permanently connected to a computer network that is directly or indirectly connected to the Internet or by using a personal computer with a modem to connect over the telephone to a larger computer or computer network that is directly or indirectly connected to the Internet.
cable modem access. Once the connection is made, the user must communicate with the web server to download web pages or other data and view them. Web browser software is used for that purpose (for instance, Microsoft Internet Explorer). Search engines and web portals facilitate surfing the web (for instance, Yahoo).

The third actor is the author/owner of the web contents. The owner (which can be a physical person or a company) who operates the website has a registered domain name, which is a website address assigned to a specific computer that can be reached by any service provider. Domain names can be registered outside the jurisdiction in which the registrant resides. The author/owner of the web contents can have it hosted by a service provider in Canada or by one located anywhere else in the world (for instance, in a state where gambling is legal). The web contents (web pages), which include program files, reside physically on the host computer, which is called a server. It is at this location that the website contents are recorded as electronic data. The server may be located anywhere in the world. The author/owner could also have the website contents hosted by his or her own computer, which is then connected to the Internet through an ISP.

Generally, the hosting service provider requires the author/owner of the website and contents to enter into an agreement not to upload (transfer files to the ISP server's computer where the website is hosted) illegal contents (for instance, hate literature and child pornography). If this type of activity takes place, the contents will be removed and the contract will be terminated. In some countries, the service provider does not require such an undertaking. Security software may also be used to prevent unauthorized access to a website by a user (password protected).

---

7 The author, who is also called the content provider, may not be the owner of the website or its operator.

8 The website is an Internet address, which enables users to exchange digital content with a particular host. The user, as a web-surfer, uses a web browser (for example, Microsoft's Internet Explorer or Netscape Navigator), which incorporates the web's pointer standard or universal resource locator (URL) to find a particular website. It has been held that a domain name is not property and lacks physical existence. It is not located where it is registered: Easthaven v. Nutrisystem Com. Inc. (2001), 55 O.R. (3d) 334 (S.C.J.) [hereinafter Easthaven], which is discussed throughout this article.

9 A web page is a "hypertext" document created using hypertext markup language.

10 A website operator may be employed by the website author/owner to update the website. Note that bulletin boards may be used for posting messages.
Basically, individuals as users interact with the Internet either by putting information on the net (uploading) or by taking information from the net (downloading). Difficulties arise due to the fact that the Internet is open-ended, and a user or author/owner of a website can always move the website and its contents to a new host and redirect or re-route web traffic to that new host. What is more, a website can be a portal to other websites or an Internet operator can use a surrogate server that is located in another state to prevent others from tracking the originating point. The origin of information may therefore be disguised.

This brief description would be incomplete without a reference to privacy and the Internet. Web servers and content providers are able to obtain valuable marketing and other information about users that visit their websites through the use of an Internet “cookie” placed on the computer’s hard drive. With each visit by a user, personal information supplied by the user is deposited in the cookie file about the visit. Thus, a profile of the user’s interests and purchasing patterns can be obtained from this personal data. The consumer/user data is a valuable asset of the owner of the website, which can be provided to third parties for direct marketing. Security technologies, such as firewalls, anti-virus software, and encryption technology,\(^\text{1}\) are designed to protect this valuable asset as well as other information from hackers, thieves, and malicious intruders. In order to prevent the unauthorized processing of computerized personal data, some countries have adopted comprehensive legislation to regulate databases containing online information about individuals.\(^\text{12}\) Canada has done this to a very limited extent in the Personal Information Protection and Electronic Documents Act\(^\text{13}\) as this legislation does not address electronic data interchange

\(^{1}\) For example, digital signatures.


as such, but prohibits the disclosure of personal information in certain situations.

The user, as a customer, viewer, or reader visiting a website and downloading data and the ISP and its server are the actors that are most likely to be reached by laws designed to control the use of the Internet since they can usually be located physically in a particular jurisdiction. The author/owner uploading the website could also be reached if he or she can be identified and is a resident of Canada. As for transactions on the Internet, it is difficult to determine where a contract has been entered or where a tort has been committed.

The main issue is the extent to which a state can adopt and enforce laws that are effective in preventing its citizens-users from accessing websites on the Internet in order to protect them against harm that it considers important. For instance, can a foreign company executive be prosecuted in Canada for failing to filter out material that his or her company posted on its website, which is objectionable in this country? Can Canada prevent the author/owner of a website from advertising the sale of an item that is prohibited by its laws or can it prevent the publication of hate literature on the Internet? Can Canada prohibit the exchange of data between Canadian database operators and persons in other countries whether or not there exists data privacy protection? Which state can control online gambling? In other words, when can a state impose its own laws, regulations, and policies on the Internet, and how can it enforce them successfully without infringing the rights or jurisdiction of other states? At the present time, any of the Internet actors can be subjected to haphazard, uncoordinated, and often inconsistent laws, regulations, and policies by states whose citizens were not meant to be able to access a particular website and where the actors were unaware that their website was being accessed. Thus, to be successful, legal regulation and enforcement must focus on all of the actors on the Internet including, in some instances, the financial intermediaries.

In this article, an attempt will be made to answer the following questions:

- Does international law place restraints on the exercise of jurisdiction by Canada to prescribe the substantive rules of criminal and private law with respect to the use of the Internet in an international context?
- What restraints are placed upon the federal Parliament and
the provincial legislatures by the Canadian constitution in the exercise of jurisdiction to prescribe, adjudicate, and enforce laws with respect to the use of the Internet in an international context?
- How effective are present Canadian criminal and private laws that are applicable to the Internet and its actors in an international context?

RESTRAINTS PLACED BY PUBLIC INTERNATIONAL LAW ON THE EXERCISE OF JURISDICTION BY CANADA TO PRESCRIBE SUBSTANTIVE RULES OF CRIMINAL AND PRIVATE LAW WITH RESPECT TO THE USE OF THE INTERNET IN AN INTERNATIONAL CONTEXT

With the explosion of Internet use and technology and its easy access all over the world, the regulation and control of the Internet and its actors has become a priority for many states. How is this to be accomplished when the Internet is independent from geographical constraints resulting from the nature of the message transmission? Which state has the authority to regulate the Internet? In other words, what are the criteria that enable a state to prescribe rules for the Internet? Are the traditional bases of jurisdiction recognized by public international law to govern the division of legislative, judicial, and executive power among sovereign states still relevant? How can territorially based laws reach persons who operate on the Internet? If a state adopts laws applicable to the Internet in an international context, is this action improper extraterritoriality?

Traditional public international law principles that are applicable to the jurisdiction of a state to prescribe are well established. They are based primarily on territory and nationality. However, in exercising jurisdiction to prescribe, the state must not act unreasonably, especially in circumstances affecting the interests of other states. In the context of the Internet, when may Canada prescribe rules to govern persons, things, or activities that are located entirely or partially outside its territorial boundaries?

THE TERRITORIALITY PRINCIPLE

Since the Internet operates without regard for state boundaries and reaches persons located in several jurisdictions simultaneously, is territoriality still relevant as a basis for the exercise of jurisdiction in order to prescribe laws applicable to the Internet? Section 402 of
the Restatement of the Law Third, Foreign Relations Law of the United States\textsuperscript{14} declares that a state has jurisdiction to prescribe law with respect to "(i) (a) conduct that wholly or in substantial part takes place within its territory; (b) the status of persons, or interests in things, present within its territory; (c) conduct outside its territory that has or is intended to have substantial effect within its territory." The territoriality principle divides jurisdictional competence into territorial compartments over which each state has authority. It flows from the principle of the sovereign equality of states. Since territorial sovereignty enables a state to legislate freely within its own territory, equality means that no state can by its legislation infringe the sovereignty of another state. An unqualified exercise of state sovereignty in disregard of the equality of other states violates international law. Lord Macmillan succinctly declared in \textit{The Cristina}\textsuperscript{15} that "[i]t is an essential attribute of the sovereignty of this realm, as of all sovereign independent States, that it should possess jurisdiction over all persons and things within its territorial limits and in all causes civil and criminal arising within these limits." Within its own territory, a state is virtually supreme, and international law places few restraints upon the exercise of its authority.

With respect to users and service providers located and operating within the state where their servers are located, the strict territoriality principle (subjective territoriality) would clearly justify the application of local laws controlling the Internet and force an ISP to prevent persons within its territory from accessing certain websites. However, to maintain that the server where web pages are physically located is the situs that would justify prescriptive jurisdiction based on subjective territoriality without any other Internet contact with that situs would be unreasonable. A state could also forbid persons within its territory from uploading and downloading information that it considers to be harmful to its interests or to the interests of its citizens.

The territoriality principle, if applied literally, does not take into account the existence of a series of related acts that may be involved in an offence committed on the Internet, especially when it is difficult to ascertain the location of one of the actors or of the activities involved. In order to avoid the difficulties created by complex situations, the territorial principle has been refined to include the effects within the territory of the prescribing state as a basis for

\textsuperscript{14} Restatement of the Law Third, \textit{supra} note 1.

jurisdiction to prescribe. The effects principle, which is also called
the objective territorial principle, enables a state to prescribe laws
governing persons outside its territory who by their conduct cause
harmful effects within the territory. Controversy arises when the
conduct creating the damaging effect is lawful where carried out. If
an activity takes place on the Internet, a state can exercise jurisdic-
tion on such an activity provided that it has, or is intended to have,
a substantial effect within its territory. Thus, libellous statements,
hate literature, child pornography, violence, or incitement to racial
hatred and discrimination posted on the Internet by an author/
owner and accessible in a particular state could subject the author/
owner to the legislation of that state provided he or she can be
identified, particularly if the website provides interactive contacts
and targets residents of the regulating state.\textsuperscript{16} The downloading of
files in Canada, if they are intended to be accessible in this country,
would make the foreign author/owner's activities subject to Cana-
dian jurisdiction.

The application of the effects principle may give rise to conflicting
claims of jurisdiction since both the state in whose territory
the conduct occurs and the state in whose territory the effects are
produced have jurisdiction to prescribe rules of law pertaining to
the conduct. In effect, no conflict should arise where all states con-
cerned prohibit the same conduct — for instance, hate literature —
on the ground that it is detrimental to their interests. Where the
effects of the foreign conduct are felt in several states, each state
should be able to apply its own laws. There is no need for one state
to defer to the laws of the other, since they all have suffered injury
(although its nature may be different for each one of them). Fur-
thermore, some states may only be interested in regulating certain
elements of a complex situation with which other states are not
interested. The effects within the territory principle does not vi-
olate the territoriality principle since the effects themselves may
be considered as a domestic constituent element of the offence or

\textsuperscript{16} See \textit{Steamship Lotus (France v. Turkey)} (1927), P.C.I.J. Series A. no. 10 at 25 [here-
inafter \textit{Lotus}]: "the courts of many countries, even of countries which have given
their criminal legislation a strictly territorial character, interpret criminal law
in the sense that offences, the authors of which at the moment of commission
are in the territory of another State, are nevertheless to be regarded as having
been committed in the national territory, if one of the constituent elements of
the offence, and more especially its effects have taken place there." The terri-
torial principle was applied in \textit{Québec (Procureur Général) v. Hyperinfo Canada
Inc.} (2001), QCCQ, which is available at <http://www.canlii.org/qc/jug/qccq/
2001/2001qccq12076.html> [hereinafter \textit{Hyperinfo}].
activity sufficient to bring it within the scope of the laws and regulations of the enacting state. However, knowledge of the effects abroad or the objective ability to anticipate such effects should be present in order to attract penal liability.

In order to avoid excessive use of the effects principle, it has been suggested that jurisdiction should be claimed only by the state where the primary effects of the unlawful conduct are felt: "In order to determine whether the effects are primary or secondary, two factors should be considered: (1) are the effects felt in one State more direct than the effects felt in other States? (2) are the effects felt in one State more substantial than the effects felt in other States?" This suggestion would justify jurisdiction that is exercised only by states that have a legitimate interest in applying their laws and regulations to the Internet and its actors. It could also make it easier to solve conflicting jurisdictional claims. A legitimate interest would exist if the state and its residents or citizens were specially targeted by the website author/owner. The new trend, however, is to subject the effects principle to the principles of reasonableness and fairness in accommodating the overlapping and often conflicting interests of states and individual Internet actors.

THE NATIONALITY PRINCIPLE

Paragraph 2 of section 402 of the Restatement of the Law Third, which declares that a state has jurisdiction to prescribe with respect to "the activities, interests, status, or relations of its nationals outside as well as within its territory" refers to the active and passive nationality principle. The nationality of the offender or of the victim provides a good basis for the exercise of jurisdiction to prescribe with respect to all the actors involved in Internet operations, provided their identity and nationality can be ascertained. As far as Canadian citizens are concerned, it is a principle that is more effective than the territoriality principle since it does not depend upon geography. There is no need to determine the locus delicti. Thus, the ISP, the author/owner of a website, and Internet intermediaries, if Canadian citizens, could be subjected to Canadian law.

17 M. Akehurst, "Jurisdiction in International Law" (1973) 46 Br. Y.B. Int’l. L. 146 at 198.

18 See Restatement of the Law Third, supra note 1 at para. 403.

19 A.D.C. Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces" (1997-8) 4 Mich. Telecommunications and Technology L. Rev. 69, suggests that since the power to control the Internet has only the most tenuous connection to
THE PROTECTIVE PRINCIPLE

Section 402(3) of the Restatement of the Law Third refers to the protective principle when it declares that a state has jurisdiction to prescribe law with respect to "certain conduct outside its territory by persons not its nationals that is directed against the security of the State or against a limited class of other State interests." Effects within the territory of the offended state are not necessary. The protective principle is justified on the ground of self-defence since a state has a legitimate right to protect itself from the effects of harmful acts or conduct that take place abroad. Of course, if the impact of the acts or conduct abroad is within its territory, the state is therefore concerned and has the right to punish the author of such harmful acts or conduct, which brings us back to the effects principle.

The protective principle could be used by a state to regulate activities on the Internet that affect its security, for instance, preventing the disclosure of classified information, espionage, counterfeiting, falsification of documents, cyber-crime and cyber-terrorism,20 software piracy, propaganda for the enemy in wartime, intrusion in national security systems, endangering systems with viruses, and malicious tampering with government sites, provided it is possible to identify and reach the real authors of the electronic messages.

THE UNIVERSALITY PRINCIPLE

Finally, section 404 of the Restatement of the Law Third covers the universality principle according to which "[a] State has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism, even where none of the bases of jurisdiction indicated in §402 is present." This principle could justify the adoption of laws that would punish actors who encourage the commission of these international

crimes via the Internet, for instance, posting on the website instructions to make a bomb or to disseminate biological weapons or direct and public incitement to commit genocide, war crimes, or even crimes against humanity. Again, the difficulty would be to identify the author of the message and the actual location of that person for the purpose of enforcement.

CONFLICTS WITH RESPECT TO JURISDICTION TO PRESCRIBE LAW

Potential or actual conflicts of jurisdiction inevitably arise when two or more states claim or exercise exclusive jurisdiction or when they have concurrent jurisdiction to prescribe. In the case of exclusive jurisdiction claimed or exercised by two or more states, the question is whether the right to prescribe claimed by one state and denied by another exists under international law. Where concurrent jurisdiction to prescribe is recognized by all the states concerned, the question is one of priorities. In the absence of international law rules determining priorities, each state that has concurrent jurisdiction should be free to exercise it. Occasionally, self-judging rules of restraint will moderate the exercise of such jurisdiction in order to minimize or eliminate the conflict of jurisdiction. In appropriate situations, jurisdiction will be declined. However, the failure to do so does not constitute a violation of international law.

Today, when determining which of the several competing principles of jurisdiction has priority in a given situation, the emphasis should not be placed on rigid principles but rather on broader criteria that embrace principles of reasonableness and fairness in accommodating the overlapping or conflicting interests of states. Whether customary international law considers "reasonableness" as a question of discretionary comity or a limitation on jurisdiction is not yet definitely settled. In the case of the Internet, two difficulties arise: (1) some states do not regulate the Internet at all or only allow certain files or information to be accessed or posted, whereas such accessing or posting is prohibited by other states and (2) a result of these differences is that an online actor or operator may be subject to a series of conflicting laws.

CONCLUSION

The various aspects of the Internet and its effects within the territory of each of several states should be taken into consideration

21 See Restatement of the Law Third, supra note 1 at para. 403.
together with other factors, such as, for instance, the importance of the legitimate interests of the states concerned in order to determine whether a state has the right to apply to the Internet and its actors its own laws to the exclusion of those of another state. Traditional and functional approaches to choice of law problems, which are now well established, can be very helpful in determining the scope of a law or regulation. There should be no mechanical approach to jurisdiction to prescribe if international conflicts of jurisdiction are to be avoided.

In the Case Concerning the Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain), Judge Sir Gerald Fitzmaurice said:

It is true that under present conditions, international law does not impose hard and fast rules on States delimiting spheres of national jurisdiction in such matters (and there are of course others, for instance, in the field of shipping, "antitrust" legislation, etc.), but leaves to States a wide discretion in the matter. It does, however:

(a) postulate the existence of limits, though in any given case it may be for the tribunal to indicate what these are with regard to the facts of that case; and (b) involve for every State an obligation to exercise moderation and restraint as to the extent of jurisdiction assumed by its courts in cases having a foreign element and to avoid undue encroachment on a jurisdiction more properly appertaining to, or more appropriately exercisable by another State.\(^2\)

This passage, when read in connection with a passage in the Steamship Lotus (France v. Turkey) case, where it was declared that “all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction,”\(^3\) supports the view that a balancing approach based on reason, fairness, reciprocity, and a lack of arbitrariness could be used to determine the reach of laws applicable to the Internet and its actors. Since the prohibitive impact of international law upon the discretion of a state to delimit its legal competence is marginal, it is not possible to maintain that the application by a state of its national laws to the Internet and its actors on the basis of its effects within the territory constitutes a clear violation of international law. It depends upon the circumstances because effective limitations are only derived from the permissive impact of international law.

The complexity of the Internet and the difficulty in locating


\(^3\) Lotus, supra note 16 at 19.
geographically its various aspects does not permit a reliance on a single element — as is the case in the criminal field — whether it be the place of occurrence of the wrongful act, the place of conduct or wrongdoing, the place of injury, or the nationality of the wrongdoer or that of the victim. A total appraisal and a flexible evaluation of a wide range of domestic and foreign contacts and interests are needed in order to determine whether it is reasonable to assert state control. The territoriality and nationality principles must be considered along with the relevant state policies and the significance of the Internet message to all the states concerned. The approach to jurisdiction must not be mechanical but rather be adapted to reality. Since foreign cooperation is needed for effective enforcement abroad, the degree of recognition that other states would accord to the domestic law — in other words, comity as reciprocity — should also be an important factor in deciding whether or not to take action against an Internet actor.

In fact, it may be inappropriate to speak in terms of extraterritoriality of laws since the Internet operates without regard for state boundaries. A state should have jurisdiction to reach the actors involved in the Internet only if its contacts with any of them are close, substantial, direct, and weighty, taking into consideration the legitimate concerns and interests of other states. At the present, unless the actors involved in the Internet are present in, or residents of, Canada or are Canadian citizens, the only way to access activities on the Internet is through the effects within Canada. Territoriality resurfaces since the harmful effects must take place in Canada. We are back to the principle of objective territoriality, which gives Canada jurisdiction to regulate the Internet and its actors for their activities no matter where they take place. Therefore, most traditional principles of public international law with respect to the jurisdiction of states to prescribe law are still relevant.

RESTRAINTS PLACED UPON THE FEDERAL PARLIAMENT AND THE PROVINCIAL LEGISLATURES IN THE EXERCISE OF JURISDICTION TO PRESCRIBE, ADJUDICATE, AND ENFORCE PUBLIC AND PRIVATE LAWS WITH RESPECT TO THE USE OF THE INTERNET IN AN INTERNATIONAL CONTEXT

Whether the provincial or the federal government may exercise the jurisdiction that Canada is entitled to assert under international law is a question of Canadian constitutional law. The Canadian constitutional framework determines the degree to which
international law is applied in any given circumstance. It has now been well established that customary rules of international law are directly applicable in the Canadian domestic legal system, while conventional law must be enacted into law by the federal Parliament or the provincial Legislatures before it will affect private rights. Since the federal Parliament and the provincial Legislatures enjoy equal and plenary powers to legislate within their individual spheres of competence, either one may violate international law by adopting laws that are contrary to international law whether customary or conventional. Therefore, Canadian legislative bodies are free to adopt laws governing all aspects of the Internet whether or not these laws disregard the public international law customary rules governing the jurisdiction of states to prescribe laws with extraterritorial effect, although they should try to avoid doing so.

In Canada, the allocation of the authority to exercise jurisdiction to prescribe, adjudicate, and enforce laws governing the Internet in an international context is governed by the Constitution Act, which includes the Canadian Charter of Rights and Freedoms. Although the federal Parliament has the power to enact laws with extraterritorial effect, the constitution of Canada does not confer such power on the provinces. However, where legislation is in relation to a subject matter situated entirely within the province, incidental or consequential effects on extra-provincial rights will not render the enactment ultra vires. Thus, with respect to jurisdiction to prescribe, only the federal Parliament can legislate


26 Constitution Act, 1867 (U.K.), 30 and 31 Vict., c. 3 as amended.


extraterritorially. This fact means that legislation to reach the Internet, its actors, and activities outside Canada is subject to federal law if the regulation of the Internet in all its aspects falls within the categories of subjects that come within the legislative competence of the federal Parliament under the constitution.31

Since the Internet is a means of inter-provincial and international communication that provides Canadians with a continuous and regular service,32 its operation must be classified as an inter-provincial undertaking that is subject to federal jurisdiction by virtue of section 92 (10) (a) of the Constitution Act.33 This classification includes ISPs that operate inter-provincially and internationally and have network infrastructures in several provinces as well as in foreign states.34

The actors of the Internet, if present in Canada, and by virtue of such presence amenable to Canadian law, are entitled to the benefits of the rights guaranteed by section 2 (b) of the Canadian Charter of Rights and Freedoms.35 Since both the federal and provincial levels of government are bound by the Charter,36 the federal Parliament and the provincial Legislatures cannot enact laws applicable to the actors of the Internet that would be inconsistent with the Charter.

---

31 See section 91 of the Constitution Act, supra note 26. For instance, criminal law, intellectual property, works and undertakings beyond the province, regulation of trade and commerce, and legislation “for the peace, order and good government of Canada in relation to all matters not coming within the classes of subjects by this Act assigned exclusively to the Legislatures of the Provinces.”

32 For example, Re Ottawa-Carleton Regional Transit Commission (1983), 44 O.R. (2d) 560 (C.A.).

33 Constitution Act, supra note 26, s. 92 (10) (a): Local Works and Undertakings other than “other Works and Undertakings connecting the Province with any other or others of the Provinces, or extending beyond the Limits of the Province.” See Toronto v. Bell Telephone Co., [1905] A.C. 52; Capital Cities Communications v. C.R.T.C., [1978] 2 S.C.R. 141.

34 See, for example, Communications, Energy and Paperworkers Union of Canada and CITY-TV, CHUM et al., [1999] CIRBD no. 22 (inter-provincial undertaking).

35 Charter, supra note 27. Section 2 (b) provides as follows: “Everyone has the following fundamental freedoms: (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication,” “subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society” (s.1) [emphasis added]. See also ss. 7 to 15 on legal rights and equality rights. See also Hogg, supra note 29 at ch. 34.

36 Section 32.
The power of Canadian courts and administrative bodies to adjudicate and enforce is also subject to constitutional limitations in the context of private international law situations involving legally relevant foreign elements. Such limitations, which apply primarily to inter-provincial situations, require a sufficient or reasonable relation with the forum state or province. In a series of cases beginning in 1990, the Supreme Court of Canada held that, to be constitutionally valid, statutory or judicial private international law rules applicable to inter-provincial situations must conform to the principles of order and fairness. These principles, which have their source in the notions of full faith and credit and due process, held to be implicit in the Canadian constitution, were first applied to the general rules of jurisdiction of Canadian courts and the common law rules of recognition and enforcement of sister-province judgments.

In *Morguard Investments Ltd. v. DeSavoye*, the Supreme Court of Canada was of the opinion that "[i]t hardly accords with principles of order and fairness to permit a person to sue another in any jurisdiction, without regard to the contacts that jurisdiction may have to the defendant or the subject-matter of the suit." To be fair to the defendant, the court must act through fair process and with properly restrained jurisdiction. The real issue is whether the court is exercising its jurisdiction appropriately. The principles of order and fairness mean that "permitting suit where there is a real and substantial connection with the action provides a reasonable balance between the rights of the parties. It affords some protection against being pursued in jurisdictions having little or no connection with the transaction or the parties."
In *Hunt v. T. & N. plc,* the Supreme Court of Canada gave constitutional status to the principles expounded in *Morguard.* Therefore, the requirement of a real and substantial connection has become the absolute constitutional limit on judicial jurisdiction of the provincial superior courts. Whenever a defendant who is an actor of the Internet is served *in juris* or *ex juris* with the process of a court of a Canadian province, he or she may challenge the proceeding on constitutional grounds if the forum province lacks a real and substantial connection with the subject matter of the proceeding or the defendant. The requirement of a real and substantial connection places a limit on the provincial rules of procedure since the provincial power to legislate with respect to service *in juris* or *ex juris* requires some serious contacts with the province. One must therefore ask the question: which electronic links or contacts have a sufficiently real and substantial connection to justify the exercise of jurisdiction on a person, thing, or entity whose connection to the forum consists of a combination of data transmission over wires or radio waves?

With respect to the recognition and enforcement of sister-province judgments, the Supreme Court of Canada declared in *Morguard:*

Recognition in other provinces should be dependent on the fact that the court giving judgment "properly" or "appropriately" exercised jurisdiction. It may meet the demands of order and fairness to recognize a judgment given in a jurisdiction that had the greatest or at least significant contacts with the subject matter of the action. But it hardly accords with principles of order and fairness to permit a person to sue another in any jurisdiction without regard to the contacts that jurisdiction may have to the defendant or the subject matter of the suit.

The Supreme Court was of the opinion that, in the past, Canadian courts had been wrong to transpose the common law rules developed for the recognition and enforcement of foreign money judgments to the recognition and enforcement of money judgments from sister provinces. Principles of order and fairness must prevail in this area of the conflict of laws. When present, they create a type of inter-provincial comity, which requires the recognition and enforcement of the judgments of sister provinces as it "is based on the common interest of both the jurisdiction giving the judgment and the recognizing jurisdiction. Indeed, it is in the interest of the

---

41 *Hunt,* *supra* note 37.

42 *Morguard,* *supra* note 37 at 1103.
whole country, an interest recognized by the Constitution itself."\textsuperscript{43} Thus, "[i]n short the rules of comity or private international law as they apply between the provinces must be shaped to conform to the federal structure of the Constitution."\textsuperscript{44}

The relevant test in determining the appropriate forum, which is based on the principles of order and fairness, is whether there was a real and substantial connection between the province whose court gave the judgment and the subject matter of the proceeding or the defendant.\textsuperscript{45} The court must have had reasonable grounds for exercising jurisdiction if its judgment is to be recognized and enforced in other provinces pursuant to an implicit full faith and credit clause in the constitution of Canada.\textsuperscript{46} At the time, \textit{Morguard} simply modified the common law rules applicable to inter-provincial judgments by expanding the circumstances that apply when a domestic court should recognize the jurisdiction of a court from another province. Hence, when \textit{Hunt v. T. & N. plc} gave constitutional status to the principles adopted in \textit{Morguard}, it became necessary for statutory and common law rules applicable to the recognition and enforcement of judgments from sister provinces to conform to these principles.

Today, Canadian courts must, as a constitutional requirement, give full faith and credit to judgments rendered in sister provinces when the original court had reasonable grounds for exercising jurisdiction that is defined in accordance with the broad principles of order and fairness. Although there is no such constitutional requirement with respect to foreign judgments, the test of real or substantial connection has been extended to cover foreign judgments.\textsuperscript{47} As a result, a foreign judgment rendered against one of the actors of the Internet must meet the requirements of order and fairness if it is to be recognized and enforced in Canada. The test of real and substantial connection does not violate the customary rules of international law regarding the jurisdiction of Canadian courts to adjudicate with respect to a person, thing, or entity located outside Canada since it must be based on some substantial

\textsuperscript{43} \textit{Ibid.} at 1107.

\textsuperscript{44} \textit{Ibid.}

\textsuperscript{45} \textit{Ibid.} at 1108.

\textsuperscript{46} \textit{Hunt, supra} note 37 at 325.

link between the forum and the person, thing, or entity over which jurisdiction is exercised.

**Canadian Criminal Law and Private International Law Applicable to the Internet and Its Actors in an International Context**

**Criminal Law**

Is Canadian criminal law capable of applying to the activities that take place on the Internet and its actors in an international context? The basic question is whether Canada can assert jurisdiction over persons not physically within its boundaries and regulate conduct that occurs in part outside these boundaries. Four major situations present themselves. First, where an offence covered by the Criminal Code or other federal statutes is committed by an actor on the Internet, can such an actor be prosecuted in Canada in view of section 6(2) of the Code, which declares that no person shall be convicted or discharged of an offence committed outside Canada. Are the Internet and its actors inside or outside of Canada when committing offences on the Internet? Does this situation require the extraterritorial application of Canadian criminal law? Second, the Criminal Code or federal statutes may specifically include offences committed outside Canada. Again, are the Internet and its actors inside or outside of Canada when committing offences on the Internet? Third, in some cases, there is no need to consider section 6(2) of the Criminal Code since, according to the Supreme Court of Canada in *Libman v. R.*, all that is necessary to make an offence and have its perpetrator subject to Canadian law and jurisdiction is that a significant portion of the activities constituting the offence must have taken place in Canada. There must exist therefore a real and substantial link between the offence and Canada. This approach is an application of the effects principle. It solves the problem of national boundaries and extraterritoriality and the difficulties arising if the subjective territoriality principle is used. Fourth, the Criminal Code provision may apply specifically to Canadian citizens regardless of where they committed the offence.

---


50 *Libman v. R.*, [1985] 2 S.C.R. 178 (soliciting US residents by telephone), which was applied in *Hyperinfo*, *supra* note 16.

51 Criminal Code, *supra* note 20 at s. 46(3) This section is also extraterritorial in scope.
Whether the physical location of a server can be used as the situs of a criminal offence is doubtful. The problem is that, as has already been mentioned, data sent from an uploader to a server can travel around the world in data packets through randomly assigned nodes and thus be sent and received through several states on its way to the downloader. Applying *Libman*, one must concede that the realization in Canada of a particular scheme to defraud would be sufficient even if the inducement and its initiation were on the Internet somewhere in virtual space. Where the Criminal Code or another federal statutory provision contains language that gives it extraterritorial effect, activities on the Internet would be included since the scope of the provision is worldwide and is not concerned with national boundaries. Where the provision is territorial in scope and one of the actors or part of the activities on the Internet is not located in Canada, the accused, provided that he or she can be identified, would be subject to the real and substantial link test, which was developed by the Supreme Court of Canada in *Libman*. Where the offence created by the Criminal Code or other federal statute is based on Canadian citizenship, it does not matter where the offence was committed.

Should an ISP, portal, or a website author/owner be responsible under Canadian law when certain text or images that are outlawed in Canada are stored on servers somewhere else in the world where they are legal and accessible to Canadian residents? Can any of the Internet foreign actors be forced to prevent users in Canada from accessing websites containing such material through filtering or some other methods? In the criminal field, the Internet is used most often for gambling, money laundering as well as the dissemination of child pornography, hate propaganda, and defamatory libel. It can also be used to circumvent securities regulations. Let us examine some of these activities.

---

52 See *La Ligue contre le Racisme et l'Antisémitisme v. Yahoo! Inc.*, November 20, 2000, which can be accessed at <www.cdt.org/speech/international/001120yahoo france.pdf>, where a French court ruled that Yahoo must block French users from accessing its US-based online auction sale of Nazi memorabilia in violation of French criminal law. However, in *Yahoo Inc. v. La Ligue contre le Racisme et l'Antisémitisme*, 169 F. Supp. 2d 1181 (N.D. Cal., 2001), the US District Court refused to defer to the injunctive order of the French court.

Online Gambling and Money Laundering

Gambling is prohibited in Canada by the Criminal Code, unless specially authorized. This prohibition includes online gambling on the Internet, therefore, the user and the author/owner of the gambling site who is the cyber-casino operator or gaming merchant could be subjected to the provisions of the Criminal Code, provided that the alleged offences are committed in Canada as the sections of the Criminal Code prohibiting gambling have no extraterritorial effect. If the author/owner operating the online gambling site, the server for the site, and all other operations are located in a gambling-friendly state, the operator could still be committing an offence in Canada by application of the Libman test because a gambler residing in Canada is logging onto a site that is accessible here. The act of entering the bet and transmitting the information from Canada via the Internet would be sufficient to constitute a gambling activity in Canada, provided the operator of the gambling website targeted users who are resident in Canada. However, it could be argued that receiving a bet from a gambler who is a resident of Canada is not a significant aspect of the activities constituting the offence of gambling in Canada, which would subject the foreign operator of the gambling site to criminal liability since the agreement to gamble would have been concluded on

54 Criminal Code, supra note 20 at ss. 201-9.
55 See, for instance, ibid. at ss. 204, 207, and 207.1 (operation of casinos on international cruise ships, which are Canadian or in Canadian waters) and the Civil Code of Quebec, Article 2629. See also An Act Respecting Lotteries, Publicity Contests and Amusement Machines, R.S.Q. c. L-6. In Ontario, see Gaming Control Act, 1992, S.O. 1992, c. 24 as amended; Ontario Casino Corporation Act, 1993, S.O. 1993, c. 25, s. 24 as amended, which repealed the Gaming Act, R.S.O. 1990, c. G.2; Alcohol and Gaming Regulation and Public Protection Act, S.O. 1996, c. 26; Ontario Lottery Corporation Act, R.S.O. 1990, c. O.25 as amended; Ontario Lottery and Gaming Corporation Act, S.O. 1999, c. 12, which has repealed and replaced the Ontario Casino Corporation Act and the Ontario Lottery Corporation Act, as amended in 1992, see Schedule L, s. 20. See also Reference Re: Earth Future Lottery, 2002 PESCAD 8 (P.E.I.) (server located in Prince Edward Island, Canada). For gambling in general, see J.-G. Castel, Gambling Control Law in Ontario (2001).
56 3D virtual casino complete with the sights and sounds of a real casino. A virtual casino is the equivalent of placing a slot machine in every house that has a personal computer!
57 In the United States, see State of Minnesota v. Granite Gate Resorts Inc. and Kerry Rogers, 1996 W.L. 767432 (D. Minn. 1996), aff’d 568 N.W. 2d 715 (Minn. Ct. App., 1997).
the Internet, which is delocalized or in a foreign state when the money is received by the operator of the gambling site.

This question is controversial since many different opinions have been expressed as to whether the Canadian Criminal Code could be applied to foreign-based gaming operators if they are offering gambling services to Canadian residents. The Report on Gaming Legislation and Regulation in British Columbia, which was published in January 1999,58 expresses the view that there exists no Canadian criminal jurisdiction over foreign gaming operators:

The issue of jurisdiction becomes more complex where a licensed off-shore Internet operator takes bets from Canadians. The question is whether Internet-based gaming operators have a "real and substantial" connection with any jurisdiction from which bets are placed. Where the Internet-based gaming operator is operating entirely offshore (i.e. where all contracts are concluded offshore, all banking arrangements are carried out offshore and the Internet service provider is located offshore), it is unlikely that Canadian courts will be able to exert jurisdiction over the operator.

Some gaming sites use remote servers-based software applications. Other sites require users to download proprietary software applications that must be installed on the gambler's computer before he or she can play. As for methods of payment, some sites require cash for each bet, which the user pays with a credit card or some other electronic form of payment, such as a Wells Fargo automatic teller machine and check card or bank wire transfers. More recently, digital cash is used quite often. It may be purchased with a credit card from an e-cash company and can be used for a variety of purposes, including gambling, since some credit card companies as well as the bank issuing such credit cards refuse to process gambling transactions. This restriction is due in part to the fact that online gamblers who have suffered heavy losses often refuse to pay their credit card debts or even sue the credit card companies, banks, ISPs, and gambling merchants in order to recoup their losses and/or damages for the consequences of such losses on the ground that gambling is illegal where the credit card holder is resident and where he has gambled online.

It is doubtful that an ISP or a portal providing access to online casinos would be committing the offence of conspiracy abroad or

in Canada to commit an indictable offence or an offence punishable on summary conviction in Canada\textsuperscript{59} as a result of gaming activities conducted on its services, particularly if it and its servers are located in a state where gambling is lawful. Since an ISP is only an information highway or conduit that is not aware of the contents of the information and files contained or posted on the website that it is hosting and has no control over gaming activities, it would lack any \textit{mens rea}. Nor, for the same reason, could it be a party to the offence of gambling.\textsuperscript{60} However, it could be required to filter out gambling websites or to refuse to host them. For the same reasons, it is unlikely that parties who provide software and financial services (e-cash companies and Visa banks) that are necessary to process transactions on such sites could be held criminally liable for such activities.

Whether a gambler, who is using his or her own computer in, let us say, Toronto, at his or her place of residence and who from there places a bet online, commits an offence in Canada\textsuperscript{61} is also a controversial question since it could be argued that gambling takes place where the bet originates\textsuperscript{62} or where it is received, provided such places can be identified.\textsuperscript{63} Again, in light of \textit{Libman}, it would seem that the gambler has committed in Canada the offence listed in section 206(4) of the Criminal Code.\textsuperscript{64} Canada is the state that, from the point of view of the gambler who is resident in Toronto, has a real and substantial link with the offence. It is also the place where the effects of gambling are felt by the gambler, win or lose. Therefore, if the gambler logging on in Toronto, assuming that he or she can be identified, is deemed to commit the offence in Canada, the fact that some elements of the gambling took place abroad does not necessarily violate international law since, as noted previously, the effects principle recognized by international law holds that a state can prescribe a rule of law governing conduct.

\textsuperscript{59} See Criminal Code, supra note 20 at s. 465(1)(c) and (d) and 465(3) and (4).
\textsuperscript{60} See \textit{ibid.} at s. 21(2).
\textsuperscript{61} See \textit{ibid.} at ss. 206(4) and 207(3)(b).
\textsuperscript{62} Place of logging-on being Toronto.
\textsuperscript{63} Country where the author/owner of the site accepts the bet and pays the winnings, if any.
\textsuperscript{64} "Everyone who buys, takes or receives a lot, ticket or other device mentioned in subsection (1) is guilty of an offence punishable on summary conviction." See also Criminal Code, supra note 20 at section 207(3)(b) on participation in lottery scheme not authorized by section 207(1) and (2).
outside its territory that has or is intended to have substantial effect
within its territory.⁶⁵

Is visiting an Internet casino physically visiting a "common gam-
ing house or common betting house," which is prohibited under
section 201 (2) (a) of the Criminal Code? And, if so, it would follow
that the online gambler is a "found in" and therefore guilty of
an offence punishable on summary conviction. Depending upon
the circumstances, the gambler and the author/owner gaming mer-
chant could also be charged for violating section 462.31 (1)⁶⁶ of
the Criminal Code, which deals with laundering the proceeds of
crime, since gambling attracts organized crime and the proceeds
of crime could be disguised as winnings. This section of the Code
has an extraterritorial effect and could cover gaming transactions
outside Canada if online gaming is used for laundering money,
since the section includes: (1) the commission in Canada of an
enterprise crime offence as well as (2) an act or omission anywhere
that, if it had occurred in Canada, would have constituted an enter-
prise crime. "Enterprise crime" is defined as an offence against,
_inter alia_, sections 202 (betting and so on) and 206(1) (e) (money
increment schemes).

To conclude, the Canadian policy of strictly prohibiting inter-
active gambling on the Internet, which makes anyone criminally
liable who, in Canada, places or accepts a wager online, is difficult
to achieve in practice. Even if all the providers of Internet gambling
services within Canada were closed down or all ISPs and servers
located in Canada were prohibited from hosting gaming websites,
nothing could prevent a determined gambler from dialing another
server offshore. Furthermore, how could Canada secure the physi-
ical person of an accused who is not present in Canada but is a
national and resident of a state where gambling is legal and there-
fore not an extraditable offence should a treaty of extradition exist
between Canada and such a state? If those individuals involved in

⁶⁵ S.A. Williams and J.-G. Castel, *Canadian Criminal Law, International and Transna-
Trade (1988)*, at 10 et seq.; *People v. World Interactive Gaming Corp.*, New York S.C.
(1999), N.Y Misc. Lexis 425 (criminal offence in New York as a result of Inter-
net gambling with offshore gaming merchants).

⁶⁶ See also *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*,
S.C. 2000, c. 17, as amended by the *Anti-Terrorism Act*, S.C. 2001, c. 41 to cover
terrorist activities and terrorist groups. See also *B.A.K. Rider and C.V. Nakajima,
Anti Money Laundering Guide (2000).*
the gaming business remain outside of Canada, there is little that law enforcement can do.

Other Offences Committed by Using the Internet

The dissemination of child pornography,\(^67\) hate propaganda,\(^68\) and defamatory libel\(^69\) by posting it on a web page on the Internet is quite a common practice. Since the sections of the Criminal Code that make it an offence to do so are not extraterritorial in scope, it would be necessary to resort to the \textit{Libman} test in order to reach both the author of the message and the owner of the website if they were located outside Canada, especially in a place unknown. This would not be the case with respect to the user downloading the material if he or she is a resident of Canada and physically present in that country. Should ISPs be treated as publishers and, therefore, be held criminally liable for the offensive contents that users load up on web pages residing at their sites if these online providers know or ought to know the nature of the material on their system?\(^70\)

With respect to violations of human rights, in \textit{Canada (Human Rights Commission) v. Canadian Liberty Net},\(^71\) the Federal Court of Canada granted an injunction to the Human Rights Commission to restrain the conduct of the defendant, which took place outside of Canada. Having violated this injunction, the defendant was found to be in contempt of court. The Supreme Court of Canada\(^72\) supported the order since a significant part of the activities relating to the violation of the court’s order took place in Canada. This

---


\(^{68}\) Criminal Code, \textit{supra} note 20 at ss. 318-20.


fact constituted a substantial link between the offending conduct and Canada, pursuant to the Libman test.73

Cyber-terrorism

Cyber-terrorism, which must be distinguished from cyber-crime,74 uses the Internet to facilitate a number of activities, for instance, soliciting and transferring funds, purchasing goods, and seeking new members. It also uses the Internet to carry out attacks against critical infrastructures that are particularly vulnerable, for instance, transportation systems, nuclear power plants, and banking and finance institutions. By infecting with a virus or other disabling method the computer networks upon which such infrastructures rely for their continued operations, cyber-terrorists are able to shut them down often causing harm to the citizens and the state relying on them.75 Recently, Canada has adopted the Anti-Terrorism Act,76 which is relevant to cyber-terrorism although it does not specifically address this topic. This act amends a certain number of statutes including the Criminal Code.


76 Anti-Terrorism Act, S.C. 2001, c. 41. In the United States, the Patriot Act of 2001, P.L. 10756, which, in section 814, deals specifically with the deterrence and prevention of cyber-terrorism by amending US Code, Title 18, s. 1030(a)(5). See also section 1030(c)(8), which defines damage as "any impairment to the integrity or availability of data, a program, a system or information." This provision covers acts of cyber-terrorism designed to disable a protected computer, which is defined as one that is used exclusively by a financial institution or the US government or, if not used exclusively, where the conduct constituting the offence affects them, or the computer is used in interstate or international commerce and communication, no matter where it is located, if the use affects such commerce and communication (s. 1030(c)(2)).
First, the act defines "terrorist activity" by referring to several international conventions dealing with various aspects of terrorism. Second, it further defines "terrorist activity" as

(B) an act or omission, in or outside Canada,

(i) that is committed

(a) in whole or in part for a political, religious or ideological purpose, objective or cause, and

(b) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or refrain from doing any act, whether the public or the person, government or organization is inside or outside of Canada, and

(ii) that intentionally

(a) causes death or serious bodily harm to a person by the use of violence,

(b) endangers a person’s life,

(c) causes a serious risk to the health or safety of the public or any segment of the public,

(d) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (a) to (c), or

---

77 Criminal Code, supra note 20 at section 83.01 (1) on terrorist activity, para. (a). The act refers to the Convention for the Suppression of Unlawful Seizure of Aircraft, which was done at The Hague on December 16, 1970, 860 U.N.T.S. 105; the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, which was done in Montreal on September 23, 1971, 974 U.N.T.S. 177; the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, which was adopted by the General Assembly of the United Nations on December 14, 1973, 1977 Can. T.S. no. 43; the International Convention against the Taking of Hostages, which was adopted by the General Assembly of the United Nations on December 17, 1979, 18 I.L.M. 1456; the Convention on the Physical Protection of Nuclear Material, which was adopted in Vienna on 3 March 1980; the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, which is supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, which was done in Montreal on February 24, 1988, 27 I.L.M. 627; the Convention for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, which was done in Rome on March 10, 1988, 27 I.L.M. 685; the International Convention for the Suppression of Terrorist Bombings, which was adopted by the General Assembly of the United Nations on December 15, 1977; UN Doc. A/RES/52/164; and the International Convention for the Suppression of Terrorist Financing, which was adopted by the General Assembly of the United Nations on December 9, 1999, 39 I.L.M. 270.
(e) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (a) to (c) and includes a conspiracy, attempt, or threat to commit any such act or omission or take away being an accessory after the fact or counselling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law.

Cyber-terrorism is covered by the definition of “terrorist activity” in section 83.01(1)(b) of the Criminal Code. The financing of terrorism using the Internet is covered by section 83.02 of the code as well as by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and Article 2 of the International Convention for the Suppression of Terrorist Financing. Finally, section 3(1)(d) of the Security of Information Act, in particular, covers both cyber-crime and cyber-terrorism since it includes harm caused by a terrorist group. This act provides that

---

78 Criminal Code, supra note 20 at section 83.01(1)(b).
79 "Every one who, directly or indirectly, wilfully and without lawful justification or excuse, provides or collects property intending that it be used or knowing that it will be used, in whole or in part, in order to carry out
   (a) an act or omission that constitutes an offence referred to in subparagraphs (a)(i) to (ix) of the definition of "terrorist activity" in subsection 83.01(1), or
   (b) any other act or omission intended to cause death or serious bodily harm to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, if the purpose of that act or omission, by its nature or context, is to intimidate the public, or to compel a government or an international organization to do or refrain from doing any act, is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years." See also ss. 83.03 and 83.04.
81 International Convention for the Suppression of Terrorist Financing, supra note 77.
83 Ibid. at section 3(2).
For the purposes of this Act, a purpose is prejudicial to the safety or interests of the State if a person...
(d) interferes with a service, facility, system or computer program whether public or private, or its operation, in a manner that has significant adverse impact on the health, safety, security or economic or financial well-being of the people of Canada or the functioning of any government in Canada.

Where cyber-terrorism is state sponsored, it constitutes an internationally wrongful act that entails the international responsibility of the state. It is also a violation of the United Nations Charter. The victim state could respond in self-defence, and the Security Council could become seized of the matter.

Judicial Cooperation and Extradition

The Mutual Legal Assistance in Criminal Matters Act, which implements treaties on mutual legal assistance in criminal matters signed by Canada with a number of countries, is also quite relevant to offences committed through the Internet since it provides, inter alia, for the taking of evidence in Canada to be used abroad, the admissibility in Canada of evidence obtained abroad, and the collection in Canada of fines imposed abroad. Since the prosecution of criminal and quasi-criminal offences requires jurisdiction over the offence and over the person of the alleged offender, extradition of alleged or convicted offenders who are fugitives from justice for offences related to the use of the Internet is possible if the

---

87 For example, the Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, dated March 18, 1985, in force January 14, 1990, Can. T.S. no 19, esp. arts. II (scope), XVI (search and seizure), and XVII (proceeds of crime).
88 Sections 17-23.
90 Section 9.
conditions of the Extradition Act\textsuperscript{91} and the relevant provisions of a treaty of extradition between Canada and the country of refuge seeking the offender are met.\textsuperscript{92}

\textit{Recognition and Enforcement in Canada of Foreign Judgments for Penalties}

As a general rule, foreign judgments resulting in monetary penalties for the benefit of foreign states, which are imposed on the actors of the Internet, are not enforceable in Canada. To do so would constitute an infringement of local sovereignty and would involve an inquiry into the policies of the foreign state under question.\textsuperscript{93} However, section 9 of the Mutual Legal Assistance in Criminal Matters Act\textsuperscript{94} could be relied upon by a foreign state that is bound to Canada by a treaty of mutual legal assistance in criminal matters. The act allows the foreign state as a judgment creditor to recover the fine in civil proceedings instituted by it in Canada, as if the fine had been imposed by a Canadian court. The enforcing court would test the jurisdiction of the foreign court that imposed the fine as if it were a foreign money judgment and not a penal judgment. Provincial rules with respect to the recognition and enforcement of foreign money judgments would be applicable.\textsuperscript{95} Moreover, the act defines "fine" as including any pecuniary penalty determined by a court of criminal jurisdiction of a foreign state to represent the value of any property, benefit, or advantage, irrespective of its location, obtained or derived directly or indirectly as a result of the commission of an offence.\textsuperscript{96} For situations not covered by the act, the Canadian court would determine whether a foreign judgment is penal or not.\textsuperscript{97} Characterization would be by the \textit{lex fori}.\textsuperscript{98}

\textsuperscript{91} Extradition Act, S.C. 1999, c. 18, as amended, especially section 3.

\textsuperscript{92} For example, the Treaty of Extradition between Canada and the United States of America and its protocols, CTS 1991/37.

\textsuperscript{93} J.-G. Castel, \textit{Canadian Conflict of Laws} (4\textsuperscript{th} ed., 1997), at para. 95, and \textit{Huntington v. Attrill}, [1893] A.C. 150 (P.C.). However, see \textit{Ivey}, supra note 47.

\textsuperscript{94} Mutual Legal Assistance in Criminal Matters Act, R.S.C. 1985, c. 30 (4\textsuperscript{th} Supp.).

\textsuperscript{95} See the recognition and enforcement of foreign and sister-provinces judgments.

\textsuperscript{96} Mutual Legal Assistance in Criminal Matters Act, \textit{supra} note 94 at s. 9(3).

\textsuperscript{97} \textit{Rosencrantz v. Union Contractors Ltd. and Thornton} (1960), 32 D.L.R. (2d) 473 (B.C.S.C.).

\textsuperscript{98} In general, see S.A. Williams and J.-G. Castel, \textit{Canadian Criminal Law, International and Transnational Aspects} (1981), at 436 et seq.
DATA PRIVACY

In a number of states, financial and personal data protection laws provide for criminal or civil liability. For instance, any local processing of online financial or personal data by a corporation established, let us say in France, would trigger the application of the French data protection law. This assertion of legislative jurisdiction accords with the subjective territorial principle. The controversial issue is whether a foreign website operator could be prosecuted for violating such privacy laws. These laws are difficult to justify and to enforce unless the accused maintains some business presence in the enacting state. Corporations not maintaining some business presence could still be subject to such laws if they used equipment located in that state for the purpose of claim processing.

Another possibility is for the privacy laws to apply to all website operators, be they foreign or domestic, who interact with domestic users. Holding foreign operators liable would be justified on the effects territorial principle. Internet intermediaries, such as ISPs or e-commerce portals, should not be held liable where they merely serve as conduits for the information and do not participate in its exchange. In 2000, Canada adopted the Personal Information Protection and Electronic Documents Act, which does not mention electronic data interchange.\(^9\) It has no extraterritorial effect and cannot reach foreign-based organizations as defined therein. Disclosure of personal information without the consent of the person involved is restricted, which would seem to include communicating such information by any means. Canadian corporations have adopted a privacy policy and appointed a privacy officer whose duty it is to make sure that personal data is not disclosed improperly.

PRIVATE INTERNATIONAL LAW

In most situations, it is the user of the Internet who will sue those individuals maintaining a website for electronic commerce or other purposes (for example, persons or companies that advertise

\(^9\) Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, ss. 2-9 as amended and Schedule I. Sections 31 et seq. (electronic documents) provide for the use of electronic alternatives where federal laws contemplate the use of paper to record or communicate information or transactions (s. 32). In Québec, see an Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. c. P-39.1 and an Act to Establish a Legal Framework for Information Technology, S.Q. 2001, c. 32. See also Uniform Law Conference of Canada, 1993 Proceedings 198, Appendix G, Electronic Data Interchange.
goods for sale, which were bought and sold online; online gaming merchants; or those persons who posted defamatory statements on a Use Net site). Private international law rules become relevant in those cases where users/customers and website suppliers and wrongdoers are located in different jurisdictions.

A website established in a foreign state can easily be accessed by a Canadian Internet user, thereby enabling the actors involved to conclude all types of contracts online. Professional services such as legal or medical advice can be delivered on the Internet by individuals whose sites are hosted on ISPs in states where they are resident and licensed. Defamatory statements can be posted on a Use Net site and distributed to all other Use Net sites around the world. Copies of a song in violation of the copyright of the owner can be uploaded to an Internet site, re-transmitted by the ISPs to other sites worldwide, and then downloaded by countless users. The absence of boundaries, which characterizes the Internet, makes it difficult to determine where a contract was concluded or a wrongful act was committed. Since place elements often play a significant role in determining the jurisdiction of courts or the law to be applied to the facts of a case pending before them, some other elements that are characteristic of the Internet have to be taken into consideration, such as whether a website is passive or interactive. The residence or domicile of the defendant may also be difficult to discover for the purpose of service ex juris in order to establish personal jurisdiction. Addresses of the computers on the Internet are digital on the network and rarely contain geographic indications. Therefore, where a business is transacted over a computer network via a website that is accessed by a user in Ontario, one could argue that it takes place as much in Ontario as in any other province or state. Being that the location of the business transaction can occur anywhere from which the Internet can be accessed, the traditional rules of private international law applicable to offline activities may not be adequate if such activities take place online. At the outset, as in the case of the criminal law, it would seem that among all the actors involved on the Internet, an ISP or a website owner such as Yahoo, when acting as a portal, should not be held civilly liable for the activities taking place on the websites they host since they are only providing access and have no control over the contents of the electronic message. They should be treated as common carriers similar to telephone companies and should not be held responsible for the information that they carry. However, more generally, should the operators of Internet businesses be subject to the jurisdiction of
the state or province where their customers are resident rather than
that of the state or province where they or their servers are located?
The discussion that follows is limited to contract and torts issues
involving the Internet and its actors.

Jurisdiction in personam

The Internet's indifference to physical borders challenges the
notion of presence by a non-resident defendant in a forum state. In
addition, asserting personal jurisdiction by reason of Internet-
related contacts is not always easy as persons doing business on the
Internet may be subject to litigation in every jurisdiction where a
web page is accessible. How can a physical person or corporation
that maintains an Internet site on the worldwide web become
subject to the jurisdiction of the federal and provincial courts in
Canada when the site can be accessed simultaneously in many
provinces or states?

In common law Canada, the exercise of adjudicative jurisdiction
over the subject matter of the action and over the person of the
defendant must not contravene the constitutional limitations on
provincial jurisdiction that require the existence of a real and sub-
stantial connection between the forum province and the subject
matter of the action or the parties. The grounds for the exercise of
jurisdiction must constitute a real and substantial connection. An
Internet presence may have to be taken into consideration in
determining the existence of a real and substantial connection. How-
ever, web activity by itself should not be sufficient unless such
activity was directed at persons in the forum province.

In Easthaven Ltd. v. Nutrisystem.Com.Inc., which involved a dis-
pute over the ownership of a domain name, the Ontario Superior
Court had to decide whether the fact that the registrar for the
domain name of the defendant had its head office in Toronto was
sufficient to constitute a real and substantial connection between

100 See Morguard, supra note 37; Hunt, supra note 37; and Craig Broadcast Systems Inc.
v. Frank N. Magid Associates Inc. (1998), 124 Man. R. (2d) 252 (C.A.) (real and
substantial connection between the defendant and the forum province of a
kind that makes it reasonable to infer that he or she had voluntarily submitted
himself or herself to the risk of litigation in its courts); WIC Premium Television,
supra note 40.

101 Old North State Brewing Co. v. Newlands Services Inc. (1998), 58 B.C.L.R. (3d) 144
(C.A.) [hereinafter Old North State Brewing Co.].

102 Easthaven, supra note 8.
Internet and Public and Private Int'l Law Principles

Ontario and the subject matter of the action. The court found that there was no such connection. Since a domain name lacks physical existence, it cannot be located in Ontario: "A domain name is still simply a unique identifier for a particular internet site located on a particular computer. That computer may be located anywhere in the world and be unrelated to where the domain name is registered."\(^{103}\)

In coming to this decision, the court was influenced by Panavision International L.P. v. Toppen,\(^{104}\) in which the US Court of Appeals distinguished between general jurisdiction and specific jurisdiction. For a US court to exercise general jurisdiction, the defendant must be domiciled in the forum state, or his or her activities in that state must have been substantial or continuous and systematic. As for specific jurisdiction, it is governed by a three-part test:

1. The nonresident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws;
2. the claim must be one which arises out of or results from the defendant's forum-related activities and
3. exercise of jurisdiction must be reasonable.\(^{105}\)

In the present case there existed neither general nor specific jurisdiction.

The exercise of jurisdiction \textit{in personam} by a Canadian superior court will generally accord with the Canadian constitution when it is based on the defendant's submission by agreement or attornment, or on the defendant's ordinary residence within the province, or on a real and substantial connection between the subject matter of the action or the parties and the forum province. The exercise of jurisdiction might not meet the requirements of the constitution when it is based solely on the defendant's temporary presence in the province or on the plaintiff's residence\(^{106}\) or on some of the grounds for

\(^{103}\) \textit{Ibid.} at 341.

\(^{104}\) \textit{Panavision International L.P. v. Toppen}, 141 F. 3d 1316 (9th Cir. 1998) [hereinafter \textit{Panavision International}].

\(^{105}\) \textit{Ibid.} at 1320.

\(^{106}\) However, see \textit{Dennis v. Salvation Army Grace General Hospital Board} (1996), 153 N.S.R. (2d) 211 (S.C.) (where the Chambers judge seemed to believe that the residence of the plaintiff met the constitutional standard), rev'd. 156 N.S.R. (2d) 372, 14 C.P.C. (4th) 207 (C.A.), which reversed the stay that had been granted on grounds of forum non conveniens; and Black, Comment on \textit{Dennis v. Salvation Army Grace General Hospital Board} at 14 C.P.C. (4th) 222.
service *ex juris*.

However, a number of Canadian courts are prepared to exercise jurisdiction in situations in which the connections between the subject matter of the action and the forum are not substantial when fairness requires them to do so, particularly when the plaintiff is incapable of seeking relief in another forum.

In the case of service *in juris*, the court must ascertain whether it has jurisdiction, based on a real and substantial connection, before considering the application of the doctrine of *forum non conveniens*. Jurisdiction over defendants that is based on presence, residence within the province, submission, or consent (for instance, by special agreement) poses few problems.

Where there is a real and substantial connection between the defendant or the subject matter of the action and the forum, Canadian courts may assert jurisdiction over the defendant even if he or she does not consent to the jurisdiction of the court and cannot be served within the territory. The bases for this kind of jurisdiction are set out in the legislation and regulations governing the courts' procedure, which vary somewhat among the common law provincial superior courts, the territorial courts, and the federal court.

This basis of jurisdiction — which is sometimes called “service *ex juris*” or “service out” or “long-arm jurisdiction” — is derived from that which was originally exercised by the English courts, but it is no longer uniformly exercised by Canadian courts in the same way that it is by the English courts. Like the English courts, Canadian courts once required all plaintiffs wishing to serve a defendant outside the territory of the forum to obtain the leave of the court. It was appropriate to exercise caution in assuming jurisdiction over absent defendants who had not consented to the jurisdiction of the court because when other courts exercised jurisdiction on this basis

---


109 For example, Alberta, Alberta Rules of Court, r. 23; Ontario, Rules of Civil Procedure, r. 17; British Columbia, Rules of Court, r. 13.

their judgments were not recognized or enforced. As the British Columbia Court of Appeal has explained, in asserting jurisdiction the court should be “mindful of international good manners or comity” not only because absent a real and substantial connection with the matter, it is arrogant to assume jurisdiction, “but also because it cannot be in the commercial interest of Canada as a trading nation that it should acquire a reputation of enmeshing foreign merchants in lawsuits not grounded jurisdictionally on a footing generally accepted in the civilized world.”

Some provinces continue to require leave to serve a defendant outside the province. In these provinces, the court may authorize the service of the originating process upon absent defendants, provided the subject matter of the proceeding prima facie falls within the scope of the relevant rule of procedure and the applicants show that they have a reasonable cause of action or a good arguable case. However, in most provinces, where the subject matter of the proceeding falls within the scope of the relevant rule, leave is not required. Despite the breadth of the categories of cases in which leave is not required, there is still a provision for obtaining leave where the subject matter of the proceeding falls outside the scope of the rules. In Nova Scotia, the originating process may be


112 Alberta, Alberta Rules of Court, r. 30; and Newfoundland, Rules of the Supreme Court, r. O.XI.


114 For example, British Columbia, Manitoba, New Brunswick, Ontario, and Saskatchewan. “Originating process” includes a counterclaim against a person who is not already a party to the main action: Henry Grethel Apparel Inc. v. H.A. Imports of Canada Ltd. (1990), 42 C.P.C. (2d) 260 (Ont. M.C.). According to the 1998 Federal Court Rules, r. 137(1): a plaintiff may serve a defendant with the statement of claim ex juris without leave.

115 For example, British Columbia, Rules of Court, r. 13(3) and (4); Ratcliffe v. Maj
served anywhere in Canada or in the United states without leave and with leave elsewhere.116

With respect to service *ex juris* with or without leave, the subject matter of the proceeding must fall within the scope of the rules of procedure for such service.117 The court must also consider whether a reasonable measure of fairness and justice, which is sufficient to meet the reasonable expectations of the national and international communities, would be achieved if it exercised jurisdiction.118 Regardless of whether or not leave is required, the exercise of jurisdiction over an absent defendant lies within the discretion of the court. Defendants will not be forced to answer locally merely because the subject matter of the proceeding comes within the scope of the rules for service *ex juris* unless it is reasonable and convenient in all circumstances for them to do so. In other words, the forum selected by the plaintiff must be *forum conveniens*.119 Any ambiguity or doubt in the application of the rules and the exercise of discretion is to be resolved in favour of the absent foreign defendant.120

Jurisdiction over a non-resident as a result of contacts on the Internet, including the operation of a website and the use of e-mail, raises some interesting questions. To impose traditional territorial concepts of jurisdiction on commercial users of the Internet is not always appropriate since, as has already been noted, the Internet has no geographical borders. Its websites are accessible simultaneously in many locations and, generally, the information they contain is not targeted to a particular audience. A different approach

---

116 Rules of Civil Procedure, r. 10.07.


119 See: *Easthaven*, supra note 8.

may have to be devised in order to exercise jurisdiction over non-residents who are online users, whether they are suppliers or purchasers of goods or services, service providers, issuers of credit or e-cash, and so on. Should the exercise of personal jurisdiction depend upon the nature and quality of the defendant’s activities in the forum province? Can online suppliers and purchasers of goods and services be considered as carrying on business in the province or state where they reside? Does jurisdiction depend upon whether the website is passive, interactive, or commercial? For instance, can a person posting a message on a website be sued in the courts of any jurisdiction where the message may be downloaded or should the website author/owner be subject only to the courts of his or her own residence or to the courts of the place where the ISP hosting the website or the portal or server is located, if such a place can be ascertained?

Where the defendant operating a website is intentionally availing himself or herself of the privilege of doing business in the province and has purposefully directed activities to persons in that province, jurisdiction would be properly exercised as the website is commercial. As a general rule, personal jurisdiction should not be asserted solely on the accessibility of a passive website that does not target persons in the province or on the location of an ISP or server. Where the place of performance or of damage is relevant with respect to an action based on a contract or tort, except perhaps with respect to a contract for services concluded and performed online, a breach of contract or damage that results from, let us say, a libel published on a passive website or bulletin board, occurs in real space and not on the Internet somewhere in virtual space, and it is therefore relatively easy to ascertain its location for the purpose of establishing jurisdiction over a non-resident defendant. The basic question is always whether the connections or contacts with the Canadian forum are real and substantial.121

In the United States,122 the courts have classified Internet contacts
on a sliding scale of passive, interactive, and commercial, particularly for personal jurisdiction over non-resident defendants. Strictly passive Internet contacts exist when a website only provides information to Internet users (for instance, merely posting information or advertising on the Internet without targeting a particular province or state). The website operator simply provides an informational website that can be accessed by interested viewers who are browsing in the forum province or state, but it does not serve as a platform for soliciting business or conducting electronic commerce. Interactive Internet contacts occur when an Internet user can communicate by exchanging information with another user (for instance, where a defendant operates an informational website but also allows a user to exchange information with the host computer by providing an e-mail address or a toll-free number). Commercial Internet contacts exist when a defendant conducts business over the Internet with users in the forum province or state (for instance, where a contract is entered into on the Internet by the defendant with a resident of the forum province or state, which involves repeated transmission of computer files over the Internet). In this case, the two-way online communication fosters an ongoing business relationship. To establish jurisdiction, interactivity must be significant.

When this sliding scale approach does not yield any results, courts might consider resorting to the effects test, whose purpose is to recognize that even though the defendant may not have physically entered the forum province, the effects of the contents of the web page can be significant and felt there significantly. Thus, passive websites that contain defamatory material, publish a company's trade secrets, or use a mark similar to a trademark could satisfy this test, provided the plaintiff suffered harm in the forum province and the defendant aimed his or her tortious conduct at this province. In other words, as the level of interactivity on the Internet increases, so too does the likelihood of finding personal

---

in a case involving defamation on an internet bulletin board). See also Panavision International, supra note 104, with respect to jurisdictional tests: general and specific and M. Geist, "Is There a ThereThere? Towards Greater Certainty for Internet Jurisdiction" (2001) 16 Berkeley Tech. L.J.1345.

123 Cybersell, Inc. v. Cybersell, Inc., 180 F.3d 414 (9th Cir. 1999).

jurisdiction. On the other hand, the more passive a website is, the less likely that personal jurisdiction may be established.

The registration of a domain name should not be sufficient to confer personal jurisdiction over the registrant on the courts of the province or state in which registration takes place. Furthermore, where jurisdiction over the subject matter or over the defendant is based on Internet contacts, it should be limited to litigation arising from such contacts and should not give the court general jurisdiction over the defendant for actions arising from non-Internet transactions or activities. The American Bar Association in its report on *Global Jurisdiction Issues Created by the Internet* clearly indicates how important targeting is to the jurisdiction to prescribe and to adjudicate:

Today, entities seeking a relationship with residents of a foreign forum need not themselves maintain a physical presence in the forum. A forum can be "targeted" by those outside it and desirous of benefiting from a connection with it via the Internet (assuming, of course, that the foreign actor is willing to confine its target to those with access to technology, a growing but still not universal subset of any forum’s population). Such a chosen relationship will subject the foreign actor to both personal and prescriptive jurisdiction, so a clear understanding of what constitutes targeting is critical.

Maintenance of a web site, by itself, should not constitute targeting the world. There is no legal or practical reason why it should. At the other extreme, designing a website whose only, or at least primary, relevance is to the population of a single forum clearly does target that forum...

In light of fundamental jurisdictional principles, based on the premise that individuals should be able to choose whether or not they wish to become connected to any given sovereign, the critical issues are the intent of the web site sponsor and what constitutes sufficient evidence of that intent. The site itself provides the first evidence of that intent. It may contain a list of fora it intends to target and filters to block participants from other States. It may contain a list of fora it does not intend to target. But filters may be by-passed, and stated intent may not reveal reality. When transactions are involved, the best evidence of intent is the willingness to deal with persons in the forum State.

Generally, in common law Canada, service *ex juris* is permitted where relief is sought against a person domiciled, ordinarily resident, or carrying on business in the jurisdiction. A defendant...

---


126 *Global Jurisdiction Issues Created by the Internet*, report of the ABA Jurisdiction in Cyberspace Project, London, 2000, s. 2.2.

127 For example, in Alberta, Alberta Rules of Court, r. 30(c); in Ontario, Rules of Civil Procedure, r. 17.02(p).
offering goods and services for sale on a website to residents of the forum would be carrying on business in the province.

Service *ex juris* is also permitted where the proceeding is to enforce, rescind, resolve, annul, or otherwise affect a contract, to recover damages, or to obtain relief with respect to a contract that is

- made in the jurisdiction;
- by its terms or implications governed by the law of the jurisdiction;
- in which the parties agree that the local court shall have jurisdiction to entertain any proceeding in respect of the contract.

Often contracts concluded online contain a forum selection and a choice of law clause. If this is not the case, the provincial Rules of Court, as noted above, refer to a most relevant contract for the exercise of jurisdiction since, in the absence of an express choice, the Canadian choice of law rule calls for the application of the system of law that is most closely and really connected with the transaction. Jurisdiction can also be established where the proceeding is in respect of a breach committed within the jurisdiction of a contract wherever made and irrespective of the fact (if that is the case) that the breach was preceded or accompanied by a breach committed out of the jurisdiction that rendered impossible the performance of so much of the contract as ought to have been performed in the jurisdiction. This rule would cover breaches of warranties on the part of a merchant who sold goods online to residents of the forum where they were intended to be used. Where a contract is concluded online and also performed online, it is difficult to determine which court has jurisdiction unless such a contract contains a choice of jurisdiction clause or the parties to it can be localized.

128 For example, in Ontario, Rules of Civil Procedure, r. 17.02(f); in Saskatchewan, Rules of Court, r. 31 (1) (f).

129 For example, in British Columbia, Rules of Court, r. 13(8) and (9).

130 In “click wrap contracts.” See *Rudder*, *supra* note 120 (forum selection clause valid; terms of agreement not analogous to “fine print” in written contract).

131 Castel, *supra* note 93 at para. 452.

132 For example, Alberta, Alberta Rules of Court, r. 30(g); Ontario, Rules of Civil Procedure, r. 17.02(f) (iv).
Service *ex juris* is possible where the proceeding is founded on a tort committed in the jurisdiction. This situation poses the problem of determining the place of tort especially with respect to complex torts such as defamation on the web and consumer product liability. In the case of defamation, it would be necessary to know where the place of Internet publication is located. Does publication take place where it is manifested and comprehended by the reader — that is, at the place of downloading by subscribers or at the place of uploading? Is targeting required? Finally, service *ex juris* is permitted where the proceeding is in respect of a claim for damages sustained in the jurisdiction arising from a tort or a breach of contract, wherever committed. This rule completes the preceding one and overcomes the difficulties involved in determining the place of the tort. It adopts the effects test.

Depending upon the circumstances, any of these rules can easily be applied to the various actors involved in online activities. Therefore, the dissemination of defamatory statements over the Internet could give jurisdiction to the court where the damage is sustained by the plaintiff, no matter where publication has taken place, especially if the defamatory material was targeted at the forum province. This fact constitutes a real and substantial connection with the forum and is an application of the effects principle. Hence, where one website is within the jurisdiction of the court, will its operator be liable for defamatory statements contained in a non-resident second site that is linked to the first or does it give the court jurisdiction over the non-resident second site?

The assertion of jurisdiction over a non-resident defendant for the infringement or violation of intellectual property rights within or without Canada could be subject to the same rules. For instance, with respect to copyright, if the website is used mainly for general advertising and promotion without targeting residents of the

---

133 For example, British Columbia, Rules of Court, r. 13(1)(h); Ontario, Rules of Civil Procedure, r. 17.02(g).

134 See *Gutnik v. Dow Jones & Company Inc.*, [2001] V.S.C. 305 (Vic. S.C.) [hereinafter *Gutnik*] (publication where paid subscribers to interactive service were located).

135 For example, Ontario, Rules of Civil Procedure, r. 17.02(h); *Duncan, supra* note 107.

136 For example, Ontario, Rules of Civil Procedure, r. 17.02(h).

137 In the United States, see, for example, *Calder, supra* note 124 (effects test); *Edias Software International L.L.C. v. Basis International Ltd.* (1996), 947 F. Supp. 413 (D.C. Ariz.).
forum state, the court should not exercise jurisdiction. The site is passive and has no real and substantial connection with the forum. On the other hand, such connection would exist if the site were interactive or commercial and allowed Internet users to download infringing material.\(^{138}\)

In a recent case that involved, in part, the question of whether the territorial reach of the Copyright Act\(^ {139}\) extends to communications by means of telecommunications that are transmitted from host servers outside Canada, the Federal Court of Appeal held that:

[185] ... The question remains: what test for locating the communications under consideration here would be most consistent with the policy of the Copyright Act and other legal principles?

[186] In my view, a royalty may be made payable in Canada in respect of communications by telecommunication that have a real and substantial connection with Canada. I would also apply the real and substantial connection test to locating the infringing activity of authorizing a communication that occurs when a content provider posts copyright material on a host server ...

[191] ... The most important connecting factors will, I assume, normally be the location of the content provider, the end user and the intermediaries, in particular the host server. However, such a connection will surely exist when each of the end nodes, namely the content provider, the communicator of the material, and the end user, is in Canada.

[192] Indeed, I would go further and say that, since the policy of the Act is to protect copyright in the Canadian market, the location of the end user is a particularly important factor in determining if any Internet communication has a real and substantial connection with Canada. On the other hand, in the absence of an end user, the location of the server will be a weightier factor in determining whether the authorization of a communication has a real and substantial connection with Canada. The real and substantial connection test is also applicable to communication from caches and hyperlinks; the location of a cache or a linked site from which material is transmitted will provide an additional potentially connecting factor.\(^ {140}\)

---


\(^{139}\) Copyright Act, R.S.C. 1985, c. C-42 as amended.

Where websites display infringing trademarks, the infringing conduct takes place where the website is created and/or maintained and not where the trademarks can be viewed over the web. Jurisdiction can also be based on damage within the forum province if the defendant's conduct targets this province and transacted business with local residents has resulted in harmful effects there.\textsuperscript{141}

The jurisdiction of a Canadian court to restrain non-residents from operating a foreign website where the activities at the site affect residents in Canada was considered in \textit{Tele-Direct (Publications) v. Canadian Business Online Inc.},\textsuperscript{142} where the Federal Court of Canada issued an interlocutory injunction against the defendant to stop the use of the plaintiff's trademark. As the defendant continued to use the trademark on servers located in the United States, the court held that while it may not have jurisdiction to enforce its order, it did have jurisdiction to find the defendant guilty of contempt of court. The Federal Court of Canada also granted an injunction restraining the defendant, which was a corporation carrying on business in Canada, from providing access to its domain name to residents of Canada and the United States.\textsuperscript{143}

In Qu\text{\text{e}}bec, in personal actions of a patrimonial nature, Qu\text{\text{e}}bec courts have jurisdiction where the defendant out-of-province online merchant or ISP is a legal person that has an establishment in Qu\text{\text{e}}bec and a dispute arises partially over the activities of the establishment in Qu\text{\text{e}}bec and partially over the activities outside Qu\text{\text{e}}bec.\textsuperscript{144} Even if the out-of-province actor has no establishment in Qu\text{\text{e}}bec, there can still be jurisdiction over it on the basis of damage suffered in Qu\text{\text{e}}bec\textsuperscript{145} (for instance, where the user, who is a resident of Qu\text{\text{e}}bec, takes an action in the province since the damage is presumed to have occurred at his or her residence);\textsuperscript{146} if the place of fault or injurious act was in Qu\text{\text{e}}bec;\textsuperscript{147} if a contractual

\textsuperscript{141} \textit{Computer City, supra} note 5: a passive website cannot constitute a use in association with wares because no transfer is possible through that medium. The Court of Appeal stated: "It is much more sensible to apply tort principles to accommodate new technologies than to distort statutory trademark rights," at para. 16.


\textsuperscript{144} Civil Code of Quebec, Article 3148(2).

\textsuperscript{145} \textit{Ibid.} at Article 3148(3).


\textsuperscript{147} Civil Code of Quebec, Article 3148(3).
obligation was to be performed in Québec as determined by the law applicable to this question;\(^{148}\) if there was an agreement to submit all existing or future disputes between them arising out of a specified legal relationship, such as a dispute arising from an online contract, to the jurisdiction of the Québec courts;\(^ {149}\) or, finally, if the defendant submitted to the jurisdiction of the Québec courts.\(^ {150}\) However, Québec courts have no jurisdiction "where the parties, by agreement, have chosen to submit all existing or future disputes between themselves relating to a specified legal relationship to a foreign authority or to an arbitrator, unless the defendant submits to the jurisdiction of the Québec authorities."\(^ {151}\)

Residence or domicile of the website author/owner in Québec is sufficient to confer jurisdiction to the Québec courts irrespective of the place where the server is located.\(^ {152}\) However, it should be noted that Article 3136 of the Civil Code provides for exceptional jurisdiction where the Québec courts have no ordinary jurisdiction, but the dispute has a sufficient connection with Québec and the proceedings cannot possibly be instituted outside Québec or where the institution of such proceedings outside Québec cannot reasonably be required. It is unlikely that a court will use this article to exercise jurisdiction over a foreign Internet service provider or the author/owner of the website.

As in the common law provinces, any attempt to assert jurisdiction will have to meet Canadian constitutional law principles, which require that there be a real and substantial connection between the Québec court and the defendant or the subject matter of the suit.\(^ {153}\) In determining whether this test has been met, the Québec courts might consider the distinction between interactive and passive activity in Québec. If the website is commercial or interactive and specially targets Québec consumers, the Québec courts would exercise jurisdiction.

In some instances, a Québec user may wish to bring a proceeding against separate entities arising out of the same online transaction

\(^ {148}\) Ibid.

\(^ {149}\) Ibid. at Article 3148(4).

\(^ {150}\) Ibid. at Article 3148(5).

\(^ {151}\) Ibid. at Article 3148, final para.

\(^ {152}\) Ibid. at Article 3148(1), and Investor Group Inc. v. Hudson, [1999] R.J.Q. 599 (S.C.) which relied on Article 68(1) of the Code of Civil Procedure to the same effect. See also Article 3134 of the Civil Code of Quebec.

\(^ {153}\) Morguard, supra note 37; and Hunt, supra note 37.
or posting, or the online defendant in the principal action may want to bring in a third party in warranty. There is no provision in the Civil Code of Québec that states that where an action is taken against a number of co-defendants, personal jurisdiction over any of them confers jurisdiction over the others, even in circumstances in which it would be preferable to have the claims against all the co-defendants decided together, so as to avoid contradictory judgments. However, if jurisdiction exists over the online merchant or author/owner of the website but not necessarily over the other participants, the action may be so related that jurisdiction over the co-defendants would be possible under Articles 3136 and 3139 of the Civil Code. The Québec courts will also exercise jurisdiction with respect to a consumer contract or a contract of employment negotiated and concluded online if the consumer or the worker has his or her domicile or residence in Québec. This rule is adequate in order to protect the consumer and the worker. A waiver of such jurisdiction by the consumer or employee is of no effect.\(^5\)

It should be mentioned that Article 3140 of the Civil Code, which provides that "[i]n cases of emergency or serious inconvenience, Quebec authorities may also take such measures as they consider necessary for the protection of the person or property of a person present in Québec," should enable Québec courts to issue injunctions against Internet actors in order to protect Québec residents. Enforcing such injunctions, however, may be difficult if the actors that are subject to them do not reside in Québec and have no assets in the province. In the contractual field, it may be advisable to distinguish between contracts negotiated and concluded online but performed, in whole or in part, offline and those contracts that are negotiated and concluded online and also performed in their totality online. In the first case, the traditional rules of jurisdiction that are applied in the common law provinces and in Québec seem to be adequate. In the second case though, it may be better to have jurisdiction depend exclusively upon a choice of forum clause.

**Law Applicable to Online Contracts and Torts**

Once a Canadian court has exercised jurisdiction in cases containing legally relevant foreign elements involving the use of the Internet, which law will it apply? Present Canadian choice of law rules applicable to extra-provincial or international contracts

\(^{154}\) Civil Code of Quebec, Article 3149.
should not pose serious problems. In common law Canada, it is well established that the parties to a contract negotiated and concluded online can select the law that will be applicable to it provided that choice is **bona fide** and legal and there is no reason for avoiding the choice on the ground of public policy. The choice will be disregarded only if its purpose is to evade the mandatory provisions of the system of law with which the transaction, objectively, is most closely and really connected.\textsuperscript{155} Anyone doing business on the Internet should use a choice of law and of forum clause. However, it may be declared to be against the public policy of the forum and ignored if there was a lack of equality of bargaining power present between the contracting parties at the time that the transaction was entered into. This scenario is possible in the case of click wrap online contracts.\textsuperscript{156}

The choice of law may also be inferred or implied from the circumstances.\textsuperscript{157} In the absence of an express or implied choice, the courts will apply the system of law with which the transaction has the closest and most real connection.\textsuperscript{158} In selecting such a system of law, a number of factors will be taken into consideration, one of them being the place of contracting, which may not be easy to ascertain when contracts are concluded online. The law that is applicable to the contract will cover all of its aspects, including performance.

In Québec, a contract is governed by Article 3109, which deals with the law applicable to its form, and Articles 3111-13 of the Civil Code, which address the determination of the law applicable to its substance or contents. These articles refer to the law that is expressly designated by the parties or, in its absence, the law that is most closely connected to the contract in view of its nature and the attendant circumstances — it being presumed that a contract is most closely connected with the law of the state where the party who is to perform the prestation that is characteristic of the contract has his or her residence or, if the contract is made in the ordinary course of business of an enterprise, its establishment. Article 3127 of the Civil Code is also relevant and declares that injury from non-performance of contractual obligations is governed by the same law as the one applicable to the contract.

\textsuperscript{155} Castel, *supra* note 93 at para. 449.

\textsuperscript{156} However, see *Rudder*, *supra* note 120, where such a clause was upheld.

\textsuperscript{157} Castel, *supra* note 93 at para. 450.

\textsuperscript{158} *Ibid.* at para. 452.
Most of the time, a business-to-business contract that is concluded online and performed, in whole or in part, online or offline contains a choice of law clause. If not, it may be difficult to localize the parties and the contract. With respect to form, is the contract concluded where the server is located or at the place that is targeted by the offer posted on the web? As for the substance of the contract, in the absence of express choice, how is the presumption applied in the case of a contract concluded and performed online when the residence or the establishment of the party who is to perform the prestation that is characteristic of the contract is unknown? If the contract is to be performed offline, it is easier to determine the law of the state with which the act is most closely connected since the place of delivery of the goods or services will be identified in the contract.

With respect to the sale of goods to non-business users or gambling online, the Québec courts would likely characterize these transactions as consumer contracts governed by Article 3117 of the Civil Code, which states that

[1]he choice by the parties of the law applicable to a consumer contract does not result in depriving the consumer of the protection to which he is entitled under the mandatory provisions of the law of the country where he has his residence if the formation of the contract was preceded by a special offer or an advertisement in that country and the consumer took all the necessary steps for the formation of the contract in that country or if the order was received from the consumer in that country.

The same rule also applies where the consumer was induced by the other contracting party to travel to a foreign country for the purpose of forming the contract.

If no law is designated by the parties, the law of the place where the consumer has his residence is, in the circumstances, applicable to the consumer contract.

The protection given to the consumer is the application of the law of the place of his or her residence at the time of the conclusion of the contract, a law with which he or she is presumed to be familiar, so long as the connections set forth in the article to that place are present. This law is easy to determine in the case of contracts concluded online and performed offline. The Consumer Protection Act\textsuperscript{159} would be relevant only if applicable by virtue of Article 3117 of the Civil Code. For instance, in accordance with the first paragraph of Article 3117, in order for the law of the state of the gambler's residence to apply in an action against an online gaming

\textsuperscript{159} Consumer Protection Act, R.S.Q., P-40.1 as amended.
merchant for annulment of the contract, its formation must have been preceded by a special offer or advertisement in his or her state of residence and the gambler must have taken all the necessary steps for the formation of the contract in that state or the order must have been received from the gambler in that state. Information on the website by a gaming merchant does not of itself amount to publicity in every province or state where it can be read on a computer screen. Furthermore, a transaction is not concluded until the funds are approved by a financial institution and deposited into an account with the gaming merchant in a place where it is assumed that this merchant is licensed to carry on gaming operations legally. This is the case even if one has accepted the view held by some American courts that when a gambler places a bet on his or her computer, he or she creates a virtual casino in his or her home in which the gaming transaction therefore takes place. Since it is assumed that the gaming merchant has no establishment at the gambler’s residence, it is difficult to see how all the necessary steps to complete the contract took place there. This scenario does not fit with the contents of Article 3117, paragraph 1. Nor could it be said that the gambler was induced by the gaming merchant to travel to a foreign country to conclude the contract by virtue of surfing the net (virtual trip).

Hence, Articles 3112-3113 of the Civil Code would be applicable to a contract between a gambler and a gaming merchant. The presumption found in Article 3113 calls for the application of the law of the place of the establishment of the party who is to perform the prestation, which is characteristic of the contract. Clearly, a gaming merchant has the characteristic obligation when opening accounts, receiving deposits, paying the winnings, refunding and paying commissions, and acting under license. However, the presumption in favour of the law of the place of the establishment might lead to the law of jurisdiction where gambling on the net is illegal or where the gaming merchant has no license to operate.

160 Note, however, that if Québec law is applicable, a gambler, as the losing party who is an adult of sound mind, may not recover the sums paid unless there was fraud or trickery: Article 2630 of the Civil Code of Quebec. In addition, if not expressly authorized by law, the contract would be invalid: Article 2629 of the Civil Code of Quebec.


162 It is assumed that the gaming merchant has its establishment in a jurisdiction where gaming is legal and under license.
If this is the case, the presumption under Article 3113 would be rebutted and would require the application of the law of the place where the gaming merchant is licensed. The shift to the law of the place where the merchant is authorized to act is clearly the place having the closest connection with the whole transaction and should be applied as the law governing the contract.

Where the place of the establishment coincides with the place of licensing, the law of that place governs the contract whether or not it is a consumer contract. Since gambling is not illegal in that place, the contract is valid and enforceable in Québec. Public order as understood in international relations cannot be used to set it aside. Of course, a Québec court could assist a foreign country by applying its law prohibiting gambling by virtue of Article 3079 of the Civil Code, which provides that “[w]here legitimate and manifestly preponderant interests so require, effect may be given to a mandatory provision of the law of another country with which the situation is closely connected. In deciding whether to do so, consideration is given to the purpose of the provision and the consequences of its application.” However, this situation is unlikely, given the strict interpretation given to this article by the Québec Court of Appeal in Arab Bank Corporation v. Wightman et al. and its attitude in Auerback v. Resorts International Hotels Inc.

If a sale and purchase of goods or real estate online, which is to be performed offline, is not characterized as a consumer contract, Article 3114 provides that

[i]f no law is designated by the parties, the sale of a corporeal movable is governed by the law of the country where the seller had his residence or, if the sale is made in the ordinary course of business of an enterprise, his establishment, at the time of formation of the contract. However, the sale is governed by the law of the country in which the buyer had his residence or his establishment at the time of formation of the contract in any of the following cases:

- negotiations have taken place and the contract has been formed in that country;
- the contract provides expressly that delivery shall be made in that country;


165 Auerback, supra note 163.
• the contract is formed on terms determined mainly by the buyer, in response to a call for tenders.
If no law is designated by the parties, the sale of immovable property is governed by the law of the country where it is situated.
Where the sale is by auction on the Internet and no law that is applicable to it is expressly designated by the parties, Article 3115 of the Civil Code provides for the application of the law of the state where the auction takes place. This place would be difficult to find. In order to avoid the problem of determining the location of some of these factors, it is always advisable to select expressly the law applicable to these types of contracts.
It should also be noted that the 1980 United Nations Convention on Contracts for the International Sale of Goods, which is in force in Canada, may be applicable to some online contractual issues if both parties to a commercial transaction are from member states, unless the parties have opted out of its coverage. The convention does not apply to the sale of consumer goods.
The determination of the law applicable to wrongful activities on the Internet is not easy in light of the Canadian common law position, which, as a general rule, calls for the application of the law of the place where the wrongful activity occurred. Exceptions to this rule are possible with respect to wrongful activities taking place outside Canada.

---

166 With respect to contracts of employment concluded online, see Article 3118 of the Civil Code of Quebec:
The designation by the parties of the law applicable to a contract of employment does not result in depriving the worker of the protection to which he is entitled under the mandatory provisions of the law of the country where the worker habitually carries on his work, even if he is on temporary assignment in another country or, if the worker does not habitually carry on his work in any one country, the mandatory provisions of the law of the country where his employer has his domicile or establishment.
If no law is designated by the parties, the law of the country where the worker habitually carries on his work or the law of the country where his employer has his domicile or establishment is, in the same circumstances, applicable to the contract of employment.
168 See Castel, supra note 93 at para. 488.
169 Tolofson, supra note 37.
Where is the place of wrongful activity when defamatory material is posted on a website and can be downloaded and read simultaneously in more than one province or state? Since the tort of defamation can only be committed when the defamatory material is published to someone other than the victim, simply uploading and posting such material onto a passive website does not make the author/owner of the website and the ISP where the web is hosted liable as publishers until such material has been viewed or downloaded by a user.\textsuperscript{171} Thus, the place of viewing or downloading would be the place of publication and not the place where the ISP or website author/owner or server is located.\textsuperscript{172} ISPs, as mere distributors or common carriers of defamatory material, should not be subject to liability provided that they do not exercise editorial control over the content of the material placed on the websites that they are hosting and have no actual knowledge of such contents.\textsuperscript{173} It is suggested that once the defamatory material has been viewed or downloaded by someone, the tort of defamation should be located where the victim's reputation has been most injured, generally at his or her place of residence or of work, which is not necessarily at the place of publication. The law of the victim's place of residence or of work would determine the liability of the defendant.

Where defective goods are manufactured negligently in one jurisdiction, sold online, and cause damage to the purchaser/consumer in another jurisdiction, statutory rules in some common law provinces call for the application of the \textit{lex fori} if the consumer suffers a loss in the province because of the defect. This legislation does not contain choice of law rules for cases falling outside its territorial scope.\textsuperscript{174} Where there is no special legislation, the application of the place of wrongful activity is not adequate. However, by analogy, relying on \textit{Moran v. Pyle National (Canada) Ltd.},\textsuperscript{175} a Supreme Court of Canada decision dealing with jurisdiction, it could be argued

\textsuperscript{171} Reform Party of Canada \textit{v.} Western Union Insurance Co. (1999), 3 C.P.R. (4\textsuperscript{th}) 289 (B.C.S.C.), where the website had been visited by 137 users.

\textsuperscript{172} Gutnick, \textit{supra} note 134 (by analogy to jurisdiction).


\textsuperscript{174} For example, Consumer Product Warranty and Liability Act, S.N.B. 1978, c. C-18.1 as amended, s. 27.

\textsuperscript{175} Moran \textit{v. Pyle National (Canada) Ltd.}, [1975] 1 S.C.R. 393.
that the place of tort is where the injury occurred, especially where
the manufacturer, having advertised its goods on the Internet and
targeted a particular audience, could reasonably foresee that such
goods would be used or consumed where the plaintiff used or con-
sumed them. This conclusion does not contradict Tolofson since, in
this case, the Supreme Court of Canada admitted that where all the
facts and events that constitute the wrongful activity occur in one
state but the consequences of that activity are felt in another state,
the place of injury is where the tort was committed.

In Québec, according to Article 3126 of the Civil Code, the law
of the state where the injurious act occurred is applicable. However,
if the damage was suffered in another state, the law of the latter
state is applicable if the person who committed the injurious act
should have foreseen that the damage would occur there. For
instance, in the case of online gambling, the liability of a gaming
merchant would depend upon whether or not gambling was an ille-
gal act as determined by the law applicable to the gaming transac-
tion. In other words, from a civil law point of view, if the gaming
transaction (opening of the online gaming account with gaming
merchants and betting) is legal by its proper law as determined by
Québec private international law rules, the gaming merchant can-
not be held civilly liable for the adverse financial consequences
suffered by the gambler who has become addicted to gambling that
is made easy on a computer at home. However, it is questionable
whether a person who uploads defamatory information onto a site
can reasonably foresee that it may be read anywhere in the world.

Where the person who committed the injurious act and the vic-
tim have their domiciles or residences in the same state, the law
of that state applies.176 Thus, with respect to a claim brought by a
Québec online gambler against a Québec bank or Visa company,
which enabled the gambler to open an account with a foreign gam-
ing merchant and which resulted in losses to him or her, the law
of Québec would apply. However, it is hard to see what advantage
the gambler would derive from such an action since, in principle,
gaming losses cannot be recovered in Québec.177 In a class action,
unless the victims are all from the same jurisdiction, there will be
different places of injury for each victim. Thus, a Québec court
could conclude that for each victim it is foreseeable that if the
injury were to occur it would be at the victim’s residence.

176 Civil Code of Québec, Article 3126, para. 2.
177 Ibid. at Article 2630.
Article 3126 of the Civil Code is also applicable to defamation on a website as well as wrongful activities that are specific to the Internet, such as hacking. As for the liability of the manufacturer of a movable, it is governed, at the choice of the victim, by the law of the state where the manufacturer has its establishment or, failing that, its residence or by the law of the state where the movable was acquired. The difficulty lies in determining the establishment or residence of the manufacturer. Furthermore, where was the movable acquired when the purchase took place online?

The determination of the law applicable to transnational infringements of intellectual property rights on the Internet is not free from controversy. Where the infringement occurs partly abroad and partly in Canada — for instance, when a copyrighted work is uploaded onto a computer in one state and then accessed and used in several other states — should the courts apply the law of the point of origin (uploading) or that of the point of reception (downloading), which corresponds to the law of the place where the plaintiff suffered injury or the law that created the right? If the infringement took place wholly in Canada, Canadian law would be relevant. Applying Tolofson to the tort claim, it would seem that in the case of infringement of foreign intellectual property rights, Canadian courts could apply Canadian law if the resulting harm to the foreign owner of the intellectual property occurred in Canada where the downloading took place.

Recognition and Enforcement of Foreign and Sister-Province Judgments

The recognition and enforcement of foreign and sister-province judgments against defendants arising out of the use of the Internet raises some important issues particularly with respect to the jurisdiction of the courts that rendered such judgments. The application by Canadian courts in the common law provinces of the principles enunciated in Morguard means that, at common law, a judgment in personam rendered in a sister province or in a foreign state should be recognized and enforced if, inter alia, at the date of commencement of the proceeding, the original court had exercised jurisdiction over the defendant on any of the following grounds:

178 Ibid. at Article 3128.
179 For the infringement of trademark in Canada via the Internet, see Computer City, supra note 5.
180 Tolofson, supra note 37.
181 Morguard, supra note 37.
the defendant was ordinarily resident or carrying on business at a permanent place within the territory over which the court exercises jurisdiction;

- the defendant had submitted to the court's jurisdiction; and

- there was a real and substantial connection between the territory over which the court exercises jurisdiction and the subject matter of the proceeding and the defendant.

When a judgment in personam rendered in a sister province is sought to be recognized and enforced, the exercise of jurisdiction on any of these grounds is appropriately restrained and compatible with the principles of order and fairness that have been entrenched in the Canadian constitution by the Supreme Court of Canada in *Hunt v. T & N. plc.* With respect to a foreign judgment, these grounds are compatible with the demands of international comity.

From a practical point of view, in inter-provincial litigation, a defendant from a sister province should always enter an appearance and defend the Canadian action on the merits since, under *Morguard,* a default judgment would probably be enforceable throughout Canada. In international litigation, the decision as to whether or not a foreign defendant should enter an appearance and defend the Canadian action on the merits would depend upon the conflict of laws rules with respect to the recognition and enforcement of foreign judgments of the jurisdiction where the successful plaintiff would most likely seek to enforce the judgment. Whether a Canadian defendant, who is sued in a foreign state,

---

182 *Hunt, supra* note 37.

183 In *Amchem Products,* supra note 37, Justice John Sopinka, speaking for the court, adopted the following definition of comity found in the judgment of the US Supreme Court in *Hilton v. Guyot* (1895), 159 U.S. 113:

"Comity" in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and goodwill, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws.

See also *Moses v. Shore Boat Builders Ltd.,* [1994] 1 W.W.R. 112 (B.C.C.A.), where the Court of Appeal listed a wide variety of factors to be considered when deciding whether or not the action had a real and substantial connection with BC, for example, the place where the cause of action arose, the respective residences of the parties, whether the defendant conducted business in British Columbia, and so on (at 124).
should enter an appearance and defend the foreign action on the merits would depend upon whether there exists a real and substantial connection between the foreign state and the subject matter of the action or the Canadian defendant that would be recognized as a valid jurisdictional basis in Canada for the purpose of its recognition and enforcement in Canada, even if the foreign court exercised jurisdiction on a different basis.184

A real and substantial connection with the original forum province or state can be anything. It depends upon the circumstances, provided the connection used by the original court is not unfair to the parties. Certainly, the grounds for exercising jurisdiction in Canada can be used by analogy to test the jurisdiction of the original court. With respect to the Internet, in *Braintech Co. v. Kostiuk,*185 the British Columbia Court of Appeal held that the mere posting of a defamatory statement on an otherwise passive electronic bulletin board is not sufficient to enter the foreign jurisdiction and to establish a real and substantial connection with that jurisdiction. No one within that jurisdiction had read the alleged defamatory statements. The court stated:

It is apparent the "real and substantial connection" relied upon for the assumption of jurisdiction by the Texas court is the alleged publication there of a libel which affected the interests of resident present and potential investors. This is true only if the mode of communication through the Internet supports this conclusion...

From what is alleged in the case at bar it is clear Kostiuk is not the operator of Silicon Investor. It is equally clear the bulletin board is "passive" as posting information volunteered by people like Kostiuk, is accessible only to users who have the means of gaining access and who exercise that means.

In these circumstances the complainant must offer better proof that the defendant has entered Texas than the mere possibility that someone in that jurisdiction might have reached out to cyberspace to bring the defamatory material to a screen in Texas. There is no allegation or evidence Kostiuk had a commercial purpose that utilized the highway provided by Internet to enter any particular jurisdiction.

It would create a crippling effect on freedom of expression if, in every jurisdiction the world over in which access to Internet could be achieved, a person who posts fair comment on a bulletin board could be hauled before the courts of each of those countries where access to this bulletin could be obtained.


185 *Braintech,* supra note 122. See also *Old North State Brewing Co.*, supra note 101.
In the default judgment it is recited that the allegations of the Original and Amended Petitions "have been admitted." This simply reflects the convention in Texas that if a defendant who has been properly served does not appear the allegations in the petition are admitted as proven. This is a deemed admission which does not assist the respondent in establishing a real and substantial connection between the appellant and the Texas court.

In the circumstance of no purposeful commercial activity alleged on the part of Kostiuk and the equally material absence of any person in that jurisdiction having "read" the alleged libel all that has been deemed to have been demonstrated was Kostiuk's passive use of an out of State electronic bulletin. The allegation of publication fails as it rests on the mere transitory, passive presence in cyberspace of the alleged defamatory material. Such a contact does not constitute a real and substantial presence. On the American authorities this is an insufficient basis for the exercise of an in personam jurisdiction over a non-resident.\footnote{\textit{Braintech, supra} note 122 at 60-2 (D.L.R.). Compare with \textit{Gutnik, supra} note 134.}

In order to be recognized and enforced in Québec, a foreign money judgment must meet the conditions found in Articles 3155-59, 3161, 3165, and 3168 of the Civil Code. As in the rest of Canada, the most important condition is that the court of the province or state where the judgment was rendered must have had jurisdiction to do so in accordance with the Québec rules of jurisdiction.\footnote{See Civil Code of Quebec, Articles 3155(1), 3164, 3165, and 3168.} To ascertain the jurisdiction of the foreign court that rendered the judgment, Québec courts use what appears to be a triple test. First, the requirements of Article 3168 of the Civil Code, which deal with the jurisdiction of the foreign court in personal actions of a patrimonial nature, must be met. This article provides as follows:

3168. In personal actions of a patrimonial nature, the jurisdiction of a foreign authority is recognized only in the following cases:

- the defendant was domiciled in the country where the decision was rendered;
- the defendant possessed an establishment in the country where the decision was rendered and the dispute relates to its activities in that country;
- a prejudice was suffered in the country where the decision was rendered and it resulted from a fault which was committed in that country or from an injurious act which took place in that country;
- the obligations arising from a contract were to be performed in that country;
- the parties have submitted to the foreign authority disputes which have arisen or which may arise between them in respect of a specific legal
relationship; however, renunciation by a consumer or a worker of the jurisdiction of the authority of his place of domicile may not be set up against him;
• the defendant has recognized the jurisdiction of the foreign authority.

Second, it is necessary to fulfill the substantial connection test of Article 3164 of the Civil Code, which declares: “3164. The jurisdiction of foreign authorities is established in accordance with the rules on jurisdiction applicable to Québec authorities under Title Three of this Book, to the extent that the dispute is substantially connected with the country whose authority is seized of the case.” This test is consistent with the constitutional requirements of a “real and substantial connection,” which are contained in Morguard, although it may be more demanding. The jurisdiction of foreign courts is established in accordance with the rules on jurisdiction applicable to Québec courts under Title Three of Book Ten of the Civil Code, which is devoted to the international jurisdiction of Québec authorities, to the extent that the dispute is substantially connected with the state whose court is seized of the case.

Third, the Québec court must determine whether the foreign court exercised its jurisdiction appropriately in light of the general dispositions of the Civil Code. For instance, a Québec court could refuse recognition of the jurisdiction of a foreign court that is otherwise competent, where, under identical circumstances, it would have declined jurisdiction on the basis of forum non conveniens. If the exercise of jurisdiction by the foreign court over an Internet user defendant meets these tests, it will be recognized in Québec.

With respect to delictual liability, where a resident of Québec does something on the Internet that causes prejudice to a user in a foreign state, it will be difficult for the foreign resident plaintiff who obtained a judgment in that state to enforce it in Québec since Article 3168(3) of the Civil Code declares that for the jurisdiction of the foreign court to be recognized, the prejudice must have resulted from a fault or injurious act that took place in that state. It is hard to imagine such a situation. However, where the prejudice

188 Morguard, supra note 37; and Hunt, supra note 37.
189 This has been called the mirror principle. See H.P. Glenn, Droit international privé in La Réforme du Code Civil (1993), vol. 3, 769-71, paras. 116-18.
190 Civil Code of Québec, Articles 3134 and 3140.
and the fault or injurious act causing it all took place in the state of the original court, such contracts would be sufficient to pass successfully the first two Québec tests of jurisdiction of the foreign court. The jurisdiction of the court of residence of the consumer could also be recognized in the context of an online consumer contract by virtue of Articles 3149 and 3164 of the Civil Code, provided there is a substantial connection with the foreign state even where the contract provides for a selection of another forum. Whether the doctrine of *forum non conveniens* can be used in this context is improbable.

With respect to class actions resulting in a foreign judgment against, for instance, an online merchant or provider of services, what matters is the jurisdiction over the defendant and not the residence of the members of the class unless it is a class action based on consumer contracts. Thus, where a class action against an online merchant or provider of services is transnational, including customers from many different provinces or states, it is likely that the decision of the court of the province or state where most customers reside would be binding on customers resident elsewhere by virtue of Articles 3136 and 3164 of the Civil Code.

What constitutes submission to the jurisdiction of a foreign court is determined according to Québec law. The test is subjective. As in the common law provinces, in the absence of a forum selection clause, a Québec or foreign online merchant with assets in Québec, if sued outside Québec, will have to decide whether or not to appear and defend the action on the merits, since if the merchant does appear, the foreign court may acquire jurisdiction over it in the eyes of Québec law. If the Québec or foreign online merchant does not appear and defend the action, a judgment by default would be given against it which may be enforceable in Québec, provided the foreign court had jurisdiction over the merchant, according to Québec law.

*Recognition and Enforcement of Foreign Judgments Based on Foreign Public Laws*

In the United States, some judgments involving activities on the Internet could be based on public laws, such as the Racketeer

192 Civil Code of Quebec, Article 3168(5).
193 See *Cortas Canning*, supra note 191.
194 Civil Code of Quebec, Article 3156.
Influenced and Corrupt Organization Act,\textsuperscript{195} which provides for civil remedies\textsuperscript{196} enabling a plaintiff who has suffered injury to obtain relief in the form of treble damages. If the foreign judgment granting such damages meets the conditions of recognition and enforcement of foreign money judgments in the common law provinces or in Québec,\textsuperscript{197} such judgment is enforceable anywhere in Canada.\textsuperscript{198} The treble damages aspect (which is close to exemplary or punitive damages) is not necessarily against Canadian public policy nor is it penal since these damages are for the benefit of a private litigant.\textsuperscript{199}

\textit{Recognition and Enforcement of Foreign Arbitral Awards}

In the common law provinces\textsuperscript{200} and at the federal level,\textsuperscript{201} the conditions for recognizing and enforcing foreign arbitral awards settling claims of a civil or commercial nature arising from the use of the Internet are to be found in special legislation that incorporates the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention)\textsuperscript{202} and the 1985 UNCITRAL Model Law on International Commercial Arbitration.\textsuperscript{203}

\textsuperscript{195} Racketeer Influenced and Corrupt Organization Act, (RICO), 18 U.S.C., s. 1961 et seq.
\textsuperscript{196} Ibid. at s. 1964 (c).
\textsuperscript{197} By analogy to Article 3079 of the Civil Code of Quebec, which allows Québec courts to apply foreign laws of immediate application.
\textsuperscript{199} Note that in Cortas Canning, supra note 191 at 1239-41, in an \textit{obiter dicta}, the Québec Superior Court was of the opinion that a foreign judgment rendered by default for an amount so disproportionate with amounts rendered in similar situations in Québec, could be said not to be in conformity with public order as understood in international relations. In Beals, supra note 184, a Florida default judgment based on private law which granted punitive damages to the plaintiffs was held enforceable in Ontario.
\textsuperscript{200} For example, International Commercial Arbitration Act, R.S.O. 1990, c. I.9.
\textsuperscript{201} United Nations Foreign Arbitral Awards Convention Act, R.S.C. 1985, c. 16 (2\textsuperscript{nd} supp.); Commercial Arbitration Act, R.S.C. 1985, c. 17 (2\textsuperscript{nd} supp.) as amended.
In Québec, such recognition and enforcement is dealt with in Articles 948-951.2 of the Code of Civil Procedure,\textsuperscript{204} which to a great extent incorporates the provision of the 1958 New York Convention.\textsuperscript{205} Arbitration appears to be a proper method of settlement of disputes arising from business-to-business contracts that are concluded and performed online or offline between parties of equal strength. In the case of consumer contracts concluded online and performed offline, which give rise to small claims, conciliation or mediation would be a cheaper and more effective method of settling disputes.

**CONCLUSION**

This brief survey of the relevance to the Internet of traditional public and private international law principles and rules applied in Canada indicates that, on the whole, they are quite adequate to cope with its challenges. Public international law principles and rules still provide a solid foundation for determining the jurisdiction of Canada to prescribe law covering activities on the Internet. The objective territoriality principle or effects principle is clearly the best justification for reaching such online activities, irrespective of territorial borders. Effects within the territory is also a solid foundation for jurisdiction to adjudicate. It works well in the field of private international law since it provides a real and substantial connection or contact with the forum. In the case of conflicting jurisdictional claims, the defendant can always invoke the doctrine of forum non conveniens.

Canadian courts should not be tempted to take jurisdiction over Internet users based on a place of origin approach where the source of transmission is located that is favoured by business interests or on a place of destination where goods or services are received that provides greater consumer protection. They should rely on a more nuanced, real, and substantial connection approach, taking into consideration targeting as one of its elements.

In order to avoid a multiplicity of legislative assertions of prescriptive and adjudicative jurisdiction over the Internet as well as in view of the uncertainty as to the exact limits of the effects principle, it would be advisable to adopt an international convention to regulate the various aspects of the Internet, especially its international

\textsuperscript{204} Code of Civil Procedure, L.R.Q. 1977, c. C-25 as am.

\textsuperscript{205} Ibid. at Article 948.
aspects. Short of an all-comprehensive multilateral convention, the
draft Convention on Jurisdiction and Foreign Judgments in Civil
and Commercial Matters would be a good place to start since it
takes into account the needs of electronic commerce.\textsuperscript{206} Voluntary
codes of conduct could also be adopted by ISPs and Internet mer-
chants of goods and services although self-regulation is not always
effective.\textsuperscript{207}

With respect to the contents of such an international conven-
tion, prescriptive and adjudicative personal jurisdiction should
not be asserted solely on the basis of accessibility in a province or
state of a passive website that does not target that province or state,
nor should the maintenance of a website by itself constitute target-
ing and subject the operator of such a site to global jurisdiction.

With respect to electronic commerce, absent fraud, forum
selection, and choice of law, clauses in online contracts should
be enforced in business-to-business transactions. In business-to-
consumer contracts, any power imbalance between them may mili-
tate against enforcing such clauses unless the consumer bargained
with the seller of the goods (which is seldom the case since most
consumer contracts are drafted by the seller and are not negoti-
able)\textsuperscript{208} or the provisions are reasonable although they are part
of a contract of adhesion. Alternative dispute resolution, such as
arbitration, should be encouraged with respect to business-to-
business online transactions. It would not be an appropriate
method of resolution of disputes with respect to small claims by
consumers, which could be resolved by conciliation or mediation.

\textsuperscript{206} A preliminary draft convention adopted by the Special Commission in October
1999 and revised in June 2001. It is available online at <http://hcch.net/doc/
jdgm2001draft-e.doc>. See Articles 6-10. See also Preliminary Document no.
12, Summary of Discussions on Electronic Commerce and International Juris-
diction, Ottawa, February 28 to March 1, 2000, by C. Kessedjian (2000), and
Preliminary Document no. 17, The Impact of the Internet on the Judgments
Project: Thoughts for the Future by A. Haines (2002), which are available at
<http://www.hcch.net/e/workprog/jdgm.html>.

\textsuperscript{207} For instance, codes of conduct for multinational corporations have not been
enforced very successfully due to their private nature.

\textsuperscript{208} Clickwrap licence agreements. However, see Rudder, \textit{supra} note 20. Note that in
\textit{Specht v. Netscape Communications Corp.}, 150 F. Supp. 2d (S.D.N.Y. 2001), the US
Federal District Court for the Southern District of New York held that Netscape’s
"smart Download" end-user licence agreement was not enforceable because the
users who downloaded the software were not required to assent to the licence
agreement. Thus, browse wrap agreements commonly used on many websites
may not be enforceable in the absence of an unambiguous act of assent.
Since global electronic commerce is here to stay, there is a need for uniform substantive rules to provide a solid legal infrastructure supporting commercial activities on the Internet. The question is who sets the rules for the Internet and how are they to be enforced? Perhaps the Internet should develop its own regulatory structures, which, in time, would lead to a separate body of customary law, such as the law merchant. Until this is done, Canadian traditional principles of criminal and private law (common law and civil law) are fairly adequate to deal with most aspects of this new technology.

209 Unidroit or UNCITRAL are the proper agencies for preparing such uniform laws. For minimalist legislation, see, for example, UN Model Law on Electronic Commerce, 1996, which is available at <http://www.unidroit.org/en-index.htm>; 1999 Uniform Law Commission of Canada, Uniform Electronic Commerce Act, 1999 Proceedings 380; US Uniform Electronic Transactions Act, 1999, which is available at <http://www.law.upenn.edu/library/ulc/ulc.htm>. These model laws are not comprehensive and do not address private international law issues. However, in the field of contracts, they indicate the time and place of sending and receipt of electronic documents (Can. Uniform Law, s. 23).

Summary

The Internet in Light of Traditional Public and Private International Law Principles and Rules Applied in Canada

This article addresses the problems related to the use of the Internet in Canada in an international context. Does international law allow Canada to regulate the Internet and its actors even if they are located abroad? Under the constitution, which level of government has the authority to do so? In which circumstances have the courts in Québec and in the common law provinces personal jurisdiction over persons using the Internet in an international context and which law do these courts apply? When are Canadian courts prepared to recognize and enforce foreign judgments involving the Internet and its actors? The author deals with these questions and is of the opinion that in most situations the federal Parliament has the jurisdiction to prescribe and the Canadian courts have the jurisdiction to adjudicate with respect to the Internet and its actors in an international context without violating international law. However, to avoid conflicts of jurisdiction, it would be better to adopt an international convention covering the various aspects of the Internet.