THE CYBERSPACE IS NOT A "NO LAW LAND"

A STUDY OF THE ISSUES OF LIABILITY FOR CONTENT CIRCULATING ON THE INTERNET

by

MICHEL RACICOT
MARK S. HAYES
ALEC R. SZIBBO
PIERRE TRUDEL

prepared for

Industry Canada

February 1997

NOTE

The views expressed in this Study are those of the authors and do not necessarily reflect government policy.

The study may be freely accessed on, and downloaded from, Industry Canada's Strategis site, which provides information on where to purchase printed copies (306-page English versions cost $15 plus taxes and shipping). Please consult: **http://strategis.ic.gc.ca/nme** [in English] or **http://strategis.ic.gc.ca/nmd** [in French].

Canadian Cataloguing in Publication Data

Main entry under title:

The cyberspace is not a "no law land": a study on the issues of liability for content circulating on the Internet.

Issued also in French under title: L'espace cybernétique n'est pas une terre sans loi. Includes bibliographical references.
Issued also on Internet.
Cat. no. C2-312/1997E ISBN: 0-662-25489-9

1. Computer network --Law and legislation.
2. Internet (Computer network). 3. Copyright.
4. Industrial Property 5. Computer crimes.
6. Intellectual property. 7. Torts -- Canada.
I. Racicot, Michel. II. Hayes, Mark S. (Stuart).
III. Szibbo, Alec R. IV. Trudel, Pierre (1952 -).
V. Canada. Industry Canada
VI. Title: A study on the issues of liability circulating on the Internet.

KE452.C6C9214 1997 343.09'99 C97-980120-6

Cat. No.: C2-312/1997E
ISBN: 0-662-25489-9

INTERNET CONTENT-RELATED LIABILITY STUDY

INTERNET CONTENT-RELATED LIABILITY STUDY

SUMMARY

1. INTRODUCTION

The Internet technology revolution, like the industrial revolution, is reshaping the world and creating new paradigms in the social, cultural, economic and political domains. People using computers can now communicate with each other across the world almost instantaneously and exchange goods and services without time nor space barriers and with less intermediaries than was the case before.

The Information Highway Advisory Council (IHAC) examined the challenges posed by this new environment in its report entitled Connection Community Content : the Challenge of the Information Highway, but, from a legal point of view, only addressed the issue of copyright liability and only that of owners and operators of bulletin board systems. In the Internet content distribution chain, more than operators and owners of BBSs are involved and more than copyright infringement is at stake.

The IHAC also recommended that the federal government should take immediate steps to lead in the development of legislative measures to clarify the question of liability of owners, operators and users of bulletin boards, Internet and Usenet sites.

Before deciding on whether legislative measures where needed, Industry Canada determined that it was best to first conduct an investigation as to what the state of the law is.

In this context, Industry Canada commissioned persons knowledgeable in these fields of law to conduct this study.

The study was not done in isolation. Some two hundred stakeholders were invited to participate by way of written submissions or in attending focus groups held in Vancouver, Toronto and Montréal.

The study appears to be the first of its kind in the world on the specific legal issues of liability for content circulating on the Internet.

The Terms of Reference specifically prohibited the authors from elaborating policy options or formulating recommendations for legislative amendment. They also prohibited any examination as to whether Internet activities should be regulated under telecommunications or broadcasting legislation.

2. THE CRIMINAL CODE AND THE INTERNET

The Criminal Code of Canada deals with many illegal activities which can be conducted on the Internet such as those related to obscenity, child pornography and hate propaganda. The fact that these activities may be conducted using the Internet does not, as such, make them immune from the reach of the Criminal Code.

2.1 Obscenity

An obscene publication is defined as any publication whose dominant characteristic is the undue exploitation of sex, or of sex together with crime, horror, cruelty or violence. Whether a publication's dominant theme is the undue exploitation of sex is determined by reference to a "community standards test" within the context of the work as a whole.

The Criminal Code creates three distinct offences:

- publication of obscene material;
- distribution of obscene material (including possession for purposes of distribution); and
- knowingly selling or exposing to public view obscene material (or having possession for such purposes).

For the first two offences (publication and distribution of obscene material), lack of knowledge that the material exceeded community standards will not be a defence unless the accused can establish due diligence, a reasonable mistake of fact or that the public good was served, since these are strict liability offences. The third offence requires the Crown to prove that the accused had a subjective knowledge of the content and nature of the obscene material in question.

Any person transmitting obscene material on the Internet could be guilty of the first offence of publication of obscene material. This would cover persons posting obscene materials to a bulletin board, Web site, newsgroup, mailing lists or on-line services.

The second offence of distribution of obscene material requires more than offering obscene material by one or more individual transactions. The case law holds that a retailer in not required to know the contents of every video, book or magazine in its store and is therefore not generally involved in distribution. On the other hand, a person that creates or copies obscene material would be deemed to be a distributor and the offence would not require proof that he/she had knowledge of the obscene material.

Thus, an operator of a newsgroup, of a BBS or of an open mailing list could be held liable for publication or distribution of obscene material especially if the BBS, newsgroup or open mailing list is moderated. Similarly, the moderator himself could be liable for publication

or distribution. Since these two offences are strict liability offences, it is also likely that an access provider could also be liable, if not for publication, at least for distribution.

The third offence (knowingly selling or exposing to public view obscene material - or having possession for such purposes) requires the Crown to prove that the accused had a subjective knowledge of the content and nature of the obscene material in question. It would, therefore, apply to any content provider, but also to moderated BBSs and newsgroups, moderated open mailing lists and to the moderator himself. Even operators of unmoderated BBSs, Web sites and open mailing lists could be held liable for exposing to public view obscene materials. However, because of the level of knowledge required, it is unlikely that access providers would be held liable. It is unlikely that a person transmitting obscene materials through a closed mailing list (or the operator of such a closed mailing list) or in a one to one e-mail would be guilty of the offence of exposing to public view in light of the "public" requirement.

2.2 Child pornography

The Criminal Code defines child pornography as including any visual representation, whether or not made electronically or mechanically, depicting a minor engaged in explicit sexual activity or having as its dominant characteristic the depiction of a minor's sexual organs or anal region, or any written material or visual representation advocating or counselling such illegal sexual activity with a minor.

In relation to child pornography, the Criminal Code prohibits three activities:

- publication, that is making, printing, publishing or possessing for the purpose of publication;
- distribution including importing, selling or possessing for the purpose of distribution; and
- simply possessing child pornography.

A person charged with any of these offences may raise defences that the acts served the public good and did not extend beyond what served the public good, reasonable mistake of fact as to the person's age or depiction of that person as a minor, artistic merit or educational, scientific or medical purposes.

The definition of child pornography is broad enough to include any computer simulated child pornography. Since the sections prohibiting child pornography are fairly recent, it is still uncertain whether these sections create strict liability offences or require proof of knowledge of the nature and content of the child pornography material. If they are held to be strict liability offences, the case law applicable in cases of production or distribution of obscene materials would apply equally to child pornography and would create a much greater burden on all those involved in the Internet content transmission chain. However, it will still

be open to the accused in such a case to avoid liability by showing that the accused exercised due diligence or reasonable care in the circumstances. If the offences are held not to be strict liability offences, the Crown will be required to prove that the accused had knowledge of the existence and nature of the child pornography.

As in the case of obscenity, a provider of child pornography posting such material to a bulletin board, Web site, newsgroup, mailing list or on-line service may be guilty of publication or distribution of child pornography. A person simply possessing child pornography in his/her computer would also be liable since possession of child pornography, unlike obscenity, is also an offence unless that person can prove that he/she had no knowledge of such material or no control over the computer.

The liability of the operators of BBSs, newsgroups, open mailing lists and Web sites, and of the access providers, will depend on whether the child pornography offences will be held to be strict liability offences or offences requiring knowledge about the existence and nature of the child pornography. If knowledge cannot be proven, the Crown may still prove the required subjective mens rea by proving recklessness or wilful blindness as to the possibility of child pornography being included in content being manipulated by such operators and by the access providers. As with obscenity, it is more likely that the operator of a moderated newsgroup, BBS or open mailing list would be found liable than in the case of an unmoderated newsgroup, BBS or open mailing list. The operator of a unmoderated mailing list may even escape conviction for possession of child pornography since possession requires both knowledge and control.

2.3 Hate propaganda

The primary legislation dealing with hate propaganda in Canada is the Criminal Code although the Federal and some of the various provincial human rights statutes and the regulations under the *Broadcasting Act* also address this issue. Only the Criminal Code was reviewed in detail for this part of the study.

The Criminal Code creates three offences:

- advocating or promoting genocide;
- inciting hatred against any identifiable group by communicating statements in any public place where such incitement is likely to lead to a breach of the peace; and
- wilfully promoting hatred against an identifiable group by communicating statements, other than in private conversation.

With respect to the first offence, the Code does not distinguish between the medium of communication used to advocate or promote genocide. Neither is it limited to a public place or communications other than in private communication. The provision contains

nothing to preclude it from applying to statements made on bulletin boards, newsgroups, mailing lists, Web sites or in e-mail communications or interactive chat sessions. However, since "advocating" or "promoting" means something active, the offence appears to be limited to the person actually making the statements. It would likely not include parties who simply enable the statements to be made via their facilities such as access providers, operators of newsgroups, mailing lists, BBS or to their moderators where the statements are made by a subscriber or user.

The second offence requires several elements to be present. First, the statements must be communicated. The definition of communicating is broad enough to include transmissions through the Internet. It appears not to be limited to the person actually making the statement and would probably extend to a third party such as an operator of an on-line service or BBS or to an access provider deliberately supplying the means or facilities for the purpose of making the statements. The definition of "statements" in this section of the Criminal Code appears to be broad enough to include communications made through Internet text, video, graphic or sound files. However, the communication of the statements must also be made in a public place. "Public place" is defined as including any place to which the public has access as a right of invitation, express or implied. It is not clear whether it means access by any member of the public or whether it would be sufficient for some members of the public to have access such as in a closed user group or closed mailing list. Finally, it is not clear whether "public place" applies only to a physical location where the public could have access, and whether it could include an electronic public place. These elements may therefore afford some avenues of defence for an accused. Finally, the offence requires that the statement communicated must incite hatred where such incitement is likely to lead to a breach of the peace. It is difficult to think of a situation where a person reading or viewing a message communicated through the Internet would be motivated to commit a breach of the peace. It is probable that the offence could be committed by persons actually making such statements, but it is less likely that it would apply to third parties who facilitate or transmit the communication, particularly if they are unaware of the specific nature of such activities.

The third offence requires someone to wilfully promote hatred against an identifiable group by communicating statements, other than in a private conversation. In contrast to the "public place" element with respect to the second offence, the language of the third offence is broader since it applies to all statements "other than in private conversation". Therefore it would appear to apply to persons posting messages to a Web site, newsgroup, bulletin board or open mailing list since these would not be likely to be considered communicated "in private conversation". However, it would appear that a message communicated by e-mail to one person only would not be indictable since it could be deemed to be a "private conversation". Messages communicated through a closed mailing list, a private bulletin board or a private interactive chat session are somewhat in between and have a greater prospect of being held to be communicated in private conversation. However, the offence also requires that the accused wilfully promote hatred against an identifiable group. Therefore, the offence would apply to persons posting messages with the intention of promoting hatred. It does not

appear however to be applicable to third parties who merely provide the means or facilities for communicating the message, even if they are aware of the contents.

3. TRADE-MARKS INFRINGEMENT AND THE INTERNET

There are three major provisions in the *Trade-Marks Act* of Canada that deal with the unauthorized use of registered trade-marks. Questions dealing with passing off and infringement of non-registered trade-marks were beyond the scope of this study.

Examination of those provisions of the *Trade-Marks Act* requires an understanding of the meaning of the expression "use" in the Act. The expression "use" has a very different meaning when it applies to goods as opposed to services. In relation to goods, a trade-mark is deemed to be used if, at the time the title to or possession of the goods is transferred, the trade-mark is: (a) marked on the goods, (b) marked on the packages in which they are distributed or (c) associated with the goods in a manner that gives notice of the association to the person to whom the property or possession is transferred at the time of such transfer. In relation to services a trade-mark is used if it is used or displayed in the performance or advertising of those services. It must be noted that, with respect to goods, utilization of a trade-mark to advertise the goods does not constitute "use" for purposes of the Act.

The Act contains three major prohibitions:

- using a registered trade-mark without the consent of the owner, in relation to those goods or services for which the trade-mark is registered;
- using a trade-mark or trade name which is confusing with the registered trade-mark in relation to the sale, distribution or advertising of any goods or services; and
- using a trade-mark registered to another person in a way that is likely to depreciate the value of the goodwill attaching to the trade-mark.

On the Internet, use of a registered trade-mark or of a confusing trade-mark or trade name is easy to establish when dealing with services. All that is required is that the trade-mark be used in the advertising of those services or, if such services are performed on the Internet, such as with a trade-mark associated with the operation of on-line services, in the performance of these services.

With respect to goods however, unauthorized use of a registered trade-mark or use of a registered trade-mark in a way that is likely to depreciate the trade-mark's goodwill requires that the trade-mark used in relation to goods appear on the goods or their packaging or be otherwise associated with the goods, at the time of the transfer of their title or their possession. It is therefore unlikely that any appearance of the trade-mark on the Internet will constitute "use" for the many goods of a tangible nature which are delivered subsequently through non-Internet facilities. However, a trade-mark could be more easily "used" on the Internet when dealing with those goods which may

be distributed through the Internet, such as software, video or music files, and similar electronic goods. Another situation of use may exist if the trade-mark appears on a contract concluded on the Internet and if the contract operates transfer of the title to the good. A trade-mark appearing in such electronic contract could thereby constitute "use" in conjunction with transfer of title in the good.

An Internet domain name may also consist of a registered trade-mark, but utilization of a registered trade-mark as a domain name may not constitute "use" as a trade-mark except if used in relation to the advertising of services or in relation to goods if used as described above in electronic goods delivered through the Internet or in an electronic contract under which title to the good passes at the time the electronic contract is concluded.

Direct infringement would be committed by the party "using" itself a trade-mark that infringes a registered trade-mark or depreciates the goodwill of a third party's trade-mark or using a confusing trade-mark or trade name. It is unclear whether other parties, who merely facilitate the posting or transmission of the infringing mark or trade name may also be liable for direct infringement. The possibility that these parties may be deemed vicariously liable or liable for contributory infringement is more likely, but still uncertain, due to the absence of relevant cases. There is also a possibility of liability for "conspiracy to infringe" if the facts substantiate a deliberate joint agreement to infringe.

4. CIVIL LIABILITY AND THE INTERNET

Each person is responsible for statements he/she makes on the Internet in the same way as he/she is responsible when making them in person, by post or by telegram, telephone, telecopier or other mode of telecommunications or in newspapers and other print media or on radio, television, cable television and other electronic media, including movies.

Because of its great versatility, the Internet can present situations analogous to all these modes of communication.

Civil liability issues arising on the Internet must be analysed in the context of the two Canadian regimes of private law: the civil law of the Province of Québec and the common law applicable in the rest of Canada. Although both regimes use very different fundamental approaches, their conclusions, when applied to a particular situation, will, in most cases, be the same.

Statutes, at both the provincial and federal levels, have also created certain statutory regimes of civil liability. By way of example, the Terms of Service of the telecommunications carriers approved by the CRTC contain provisions dealing with the carriers' liability for content transmitted over their facilities. Those provisions, in general, tend to exonerate the carriers from liability.

4.1 The Prohibited Acts

There are six principal situations which could generate civil liability on the Internet:
- defamation, libel and harm to reputation;
- invasion of privacy;
- misuse or failure to protect personal information;
- communication of erroneous information;
- violation of secrecy; and
- unfair competition.

4.1.1 Defamation

At common law, a defamation action is made up of three elements:
- offending statements made known by someone other than their author;
- the defamation refers to the plaintiff; and
- the statements are false and discredit the plaintiff.

Once proof of publication has been made, it is presumed that the statements are false, that they were intended to defame and that the plaintiff suffered damages.

In addition to the other key defences (the statements were true, the statements were fair comment, the defendant was not motivated by malice or the defendant is protected by a privilege), the "innocent dissemination" defence is the most important in the context of the Internet. Three conditions must be met for this defence to be successful:

- the defendant was innocent of any knowledge of the libel contained in the work he disseminated;
- there was nothing in the work or in the circumstances under which it came to him or was disseminated by him which ought to have lead him to suppose that it contained a libel; and
- the work was disseminated without any negligence.

The situation is essentially the same under Québec civil law although the analysis proceeds differently.

4.1.2 Invasion of privacy

Under Canadian common law, unlike the situation in the United States, there is no recognition as such of the right to privacy. The Supreme Court of Canada did recognize, starting in 1982, that the right to privacy was protected to a certain degree

by the Canadian Charter of Rights and Freedoms, at least in situations in which there was a legitimate expectation of privacy.

Four provinces have adopted Privacy Acts in Canada (Saskatchewan, Manitoba, Newfoundland and British Columbia) under which invasion of privacy is a tort for which an action can be instituted, without proof of damage, against any person who knowingly and wrongfully violates the privacy of another person. In general, these statutes are expressed in general terms and would apply to messages travelling over the Internet, with the possible exception of the Manitoba Act which covers only messages sent over the telephone.

In general, a publication is not an invasion of privacy under circumstances in which (in addition to other available defences) there is reasonable justification for believing that it contains information which is in the public interest, that it is fair comment on a matter of public interest or that it is privileged, in accordance with the rules relating to defamation.

In Québec, privacy is protected by the provisions of Articles 35 to 41 of the Québec Civil Code which protect the right to privacy and respect for one's reputation.

Under both the common law and civil law regimes, privacy cannot be recognized as absolute. The limits most likely to be encountered in the Internet context are those following from consent, freedom of expression, freedom of the press and other means of communication, maintenance of public order, public interest in information and the absence of a reasonable expectation of privacy. Since electronic environments are made up, like physical environments, of public and private places, the reasonable expectation of privacy could vary depending on the context in which the user is situated. A US court has even established that there could be no reasonable expectation of privacy in e-mail communications made by an employee to his supervisor over the company's e-mail system notwithstanding any assurances that such communications would not be intercepted by management!

4.1.3 Protection of personal information

There is a distinction between protection of the right to privacy and protection of personal information. The right to privacy has a greater scope than the concept of protection of personal information. This nuance is important on the Internet especially when operators of Web sites and on-line services start assembling information, sometimes without the knowledge of their users and subscribers, about the behaviour of those persons accessing such sites and services. In Canada, only the Province of Québec has adopted a legal regime on the gathering of personal information and the making of files on other people. These are contained in Sections 37 to 41 of the Québec Civil Code and these general provisions are complemented by

a specific statute governing the gathering, management and communication of personal information by enterprises: an *Act Respecting the Protection of Personal Information in the Private Sector*. These provisions would apply even if the Internet is used to gather such personal information.

4.1.4 Communication of erroneous information

At common law and under the Québec civil law, a person communicating information must be prudent and diligent to verify that the information provided is not erroneous especially in circumstances in which a reasonable person would know that he/she was being trusted by the person to whom the information is provided. In the context of the Internet, this is especially true of the on-line service providers and operators of data banks. Operators of services intended for the general public, with no prior contract between the information provider and the user, have an obligation to be prudent and diligent when they transmit information. If the operator is negligent and transmits erroneous information, it could be held liable for damages. In cases where the information is provided by professional data banks, the courts have demonstrated a tendency to be more severe in imposing liability standards, even going so far as to impose no-fault liability.

4.1.5 Violation of secrecy

The study does not cover the whole field of the law relating to trade secrets and fiduciary obligations. However, it is well established, both at common law and under the Québec civil law, that violation of secrecy, whether made with the help of the Internet or through more traditional means, is subject to sanction.

4.1.6 Unfair competition

Competition is legitimate under Canada's economic and legal system. However, if it becomes deceitful or otherwise ceases to be fair and honest, it is actionable both at civil law and under common law, regardless of whether such activities take place on the Internet or in more traditional "locations".

4.2 Who is responsible

The person who performs the illegal act is responsible for resulting damages. However, the Internet context raises important questions concerning the liability of all those who intervene in the Internet transmission chain of communication. The responsibility of these persons depends on their actual activities not on who they are. The best way to analyse the situation is to use metaphors comparing the conduct of the persons involved in the Internet content transmission chain with those of traditional activities, even if those activities

are described in reference to the name of a person (e.g. a publisher) rather than with the action itself. There are essentially seven metaphors:

- publisher;
- broadcaster;
- re-broadcaster;
- librarian, bookstore or news-stand;
- re-transmitter;
- space owner; and
- common carrier

4.2.1 Publisher

A publisher communicates information to third parties knowing that the information will be read, seen or heard. Voluntary publication assumes knowledge of the content of the information transmitted. In the Internet context, publication can result from the transmission of files, from electronic discussions or from making available information in files. In all these situations, the decision to publish belongs to the publisher. From such controlling power follows liability for the transmission of harmful information. Thus, if an on-line service provider exercises a degree of control over the information, it is reputed to be acting as a publisher. It may be that where control is not of an editorial nature but of a technical nature, or in order to prevent a discussion group from overflowing out of the theme it is assigned, the site operator would then not be automatically considered to be a publisher since it would exercise no editorial control *per se*.

4.2.2 Broadcaster

When they are free to broadcast, broadcasters are generally considered to be the publishers of the statements they transmit and thus have the same standards of liability as a publisher. Broadcaster liability can also result from harmful statements made by members of the public acting in their own names. An exception to this occurs if the statements are made "live" unless the broadcaster endorses them or the statements are made with the broadcaster's prior knowledge or if the broadcaster was shown to be negligent.

4.2.3 Re-broadcaster

A re-broadcaster circulates material published by others. In principle, a re-broadcaster is liable to the same extent as it would have been if it had itself published the material in the first place. Its liability, however, will be determined by its capability to verify the content of the information broadcast.

4.2.4 Librarian

Librarians, book sellers and operators of newsstands are distributors of information. Contrary to a re-broadcaster which repeats the information, these participants in the information distribution chain only deliver or provide the information. Distributors do not control the content of the information they transmit. They are, therefore, not liable if it is harmful. However, when made aware of the harmful nature of the information, distributors have the duty to withdraw it. Failing to do so, they can be held liable.

The same holds true on the Internet. An operator of an on-line service, a Web site, a BBS, if it is not moderated, could be in the same situation. It has no control over the information circulating on the system and thus cannot know or have reason to know of the harmful nature of the messages. For these reasons, it is usually not liable. However, once made aware of the harmful nature of the information, there is an obligation to take all necessary measures to prevent circulation of the harmful content or to have it withdrawn.

4.2.5 Re-transmitter

Programming distributed by cable television distribution systems, direct satellite to home broadcasting and the like do not originate with these operators which do not modify the content of the programs in any of the distributed signals. In these situations, re-transmitters are not liable for the content they re-transmit.

4.2.6 Space owner

In general, under Canadian law, space owners are not liable for the activities of their tenants or guests unless they are aware of the illegal activities of these people. However, once an owner is informed of these illegal activities, it has an obligation to act. Likewise, Internet site operators may not be initially liable for the content posted or transmitted by their users, but they have an obligation to withdraw the information once made aware that the information is illegal.

The true debate for “librarians”, “ re-transmitters” and “space owners” is to determine at what point the obligation to withdraw illegal material arises: is it when they are informed by a private complainant or an authority (including police forces) or only after a court decision pronounces that the material is illegal. We submit that this will depend on the circumstances of every case but that the liability of any intermediary would be lower if it can be demonstrated that it acted with due diligence in the circumstances.

4.2.7 Common carrier

Contrary to publishers and distributors, common carriers have the obligation to carry any message and may not discriminate against the content of the message nor against the person who sends it. Since they act only as a conduit for transporting information from one site to another, common carriers have in principle been freed of liability for the content provided by their users and subscribers. It is generally believed that when acting as common carriers, both the telecommunications carriers and the Internet access providers would enjoy the same level of immunity on the Internet. This depends, of course, on the activity actually conducted by the carrier and access provider.

In both cases, however, once made aware that information continuing to reside on the network is harmful, the telecommunications common carrier and the access provider would have the same obligation as other operators to withdraw such information (if they have the legal power to do so).

4.3 Relations between liability and control of information

An access provider, a system operator or any other actor in the Internet content transmission chain can, depending on circumstances, have different degrees of control over information. Depending on the degree of control effectively exercised, their liability would be lesser or greater. If such a distributor has physical control over the material published, it has the duty to make reasonable inquiries into the accuracy of statements alleging that such material may be potentially harmful. If such inquiries lead to the conclusion that the material would indeed be harmful, it has the obligation to withdraw it from circulation. If it fails to do so, it may be held liable.

The longevity of the information also has a direct influence on the possibility of exercising control. Liability will not be evaluated in the same way for information that is stable than for information which varies continuously. It is, in many cases, virtually impossible to revise the content of variable information or, once transmitted, to stop its circulation before damage is suffered. The liability of an operator will therefore be greater with respect to stable information than with continuously variable information.

5. COPYRIGHT INFRINGEMENT AND THE INTERNET

The *Copyright Act* defines four types of copyright works: literary, dramatic, musical and artistic. Every type of work must be included within one or more of those categories although certain subcategories such as architectural works and cinematographs also exist. The classification to which a work belongs is not always evident. For example, computer programs are classified as literary

works. In the case of a compilation containing two or more categories of works, the compilation is deemed to be a compilation of the category making up the most substantial part of the compilation.

The classification of a work has importance to the question of infringement since some types of infringement and exceptions apply to certain categories of works but not to others.

The initial owner of copyright in a work is its author except in case where the work was created in the course of employment, in which case the copyright is owned by the employer absent any agreement to the contrary.

Many creative people are using the Internet to participate in the creation of collective works. If the contribution of one author is not distinct from the contribution of the other author or authors, the work produced by the collaboration of two or more authors is known as a work of "joint authorship". Under Canadian law, each of the joint authors is, in such case, entitled to full copyright in the work, which essentially means that the work must be exploited by agreement of all of the joint authors or not at all. This is very different from the situation in the United States where a co-owner has greater liberty to act by himself.

The advent of the Internet has also raised issues dealing with the interpretation of prior licenses or assignments. In some cases it is not clear whether these prior assignments or licenses include the rights to electronic reproduction and electronic communication to the public. In this respect, freelance authors in Canada are suing newspaper and magazine publishers for copyright infringement.

The Internet is also being used to distribute digital products such as musical works. As of the writing of this study the Copyright Board is considering a tariff submitted by SOCAN for the right to communicate musical works to the public by telecommunication on the Internet. As this matter is *sub judice*, detailed comments concerning the legal justification for this tariff are not appropriate at this time.

5.1 The exclusive rights

Since copyright is a creature of statute. Since the exclusive rights enjoyed by the owner of copyright are only as contained in the *Copyright Act*, it is necessary to examine carefully the exclusive rights granted by the *Copyright Act* to copyright owners. These rights are listed in Section 3 of the Act. The rights which are the most relevant in the Internet environment are the right to produce or reproduce the work, to perform it in public, to publish it, to communicate it to the public by telecommunication and to authorize any of these acts.

The author of a work is also entitled to certain moral rights, including the right to the integrity of the work and the right to be associated with the work as its author under his/her true name or a pseudonym or alternatively the right to remain anonymous.

The Act also contains provisions dealing with indirect infringement of copyright. When dealing with infringing copies, prohibited activities are the following:

- the sale or lease of a work or the exposure or offer for sale or hire;
- the distribution for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright;
- the exhibition of a work in public by way of trade; or
- the importation of the work into Canada for sale or hire.

In order for there to be indirect infringement, there must be knowledge on the part of the infringer that the work infringes copyright or would infringe copyright if copies had been made within Canada. Of note, the activities covered are generally, but not exclusively, commercial in nature.

The various rights granted to the owner of a copyright work may be assigned or licensed to different persons. In addition, a given activity may involve the infringement of more than one of the exclusive rights of the copyright owner.

The *Copyright Act* does specify certain exclusions which prevent some of these potential multiple infringement scenarios. In particular, the Act specifies that the communication of a work to the public by telecommunication is neither a performance in public, nor the authorization of a performance in public of the work.

It is important to identify which of the exclusive rights are being infringed by Internet communications for two main reasons. First, there may be defences available for some categories of infringement, but not to others. Second, as noted above, the exclusive rights may have been assigned or licensed to different entities. For example, a composer or a publisher of a musical work would generally assign performance and telecommunication rights and reproduction rights to separate collectives for the purpose of copyright administration.

In order to evaluate the nature of copyright infringement on the Internet, it is useful to break down common Internet transactions into two main categories:

(i) those involving e-mail and newsgroups; and
(ii) those involving the World Wide Web, FTP and BBSs.

5.2 E-mail and newsgroups transactions

Electronic mail is by far the most common use of the Internet: a single user originates a message to which text, software, pictures, videos or music may be attached and the message together with its attachments is delivered to one or more users on the Internet.

Newsgroups must be considered along with e-mail because they are similarly message-based except that they involve the public posting of a sender's message and any attached files in one or more of thousands of newsgroups categories. Responses may be made by posting a responding message to the newsgroup or by sending an e-mail message directly to the user who posted the original message.

The transmission of a work by an Internet e-mail message is a communication of the work by telecommunication. But for such a transmission to infringe the communication right, it must also be a communication "to the public".

The Information Highway Advisory Council ("IHAC") Copyright Subcommittee expressed the opinion that "point-to-point e-mail between two individuals, even where it includes a copyright work, is not a communication of that work to the public". However, at some point the number of recipients of an e-mail is so large that the communication is "to the public". No criteria have yet been developed by which it could be determined how large the number of recipients of an e-mail message must be before the message is deemed to be sent "to the public", but it may be that the method by which the intended recipients are selected will be determinative. For example, a personal e-mail mailing list compiled by an individual over time may still be private despite the number of recipients. However, a broadcast message to all persons with an e-mail address with a specific suffix would appear to be a communication to the public since the sender is targeting a wide group of recipients not individually identified. Such a "public broadcast message" may very well be directed to fewer recipients than a "private" e-mail message sent to a large private mailing list. It is the originator's state of mind that is decisive and determining whether the communication will be private. At the opposite end of the spectrum, the posting of a message to a newsgroup involves a potential communication to an undetermined number of persons not known to the sender and therefore constitutes a communication to the public.

In the case of an e-mail or newsgroup transmission, the right of reproduction will also be infringed in the intermediate steps involved in getting the message from the sender to the recipients. First, the sender may make a reproduction in preparing to send the message, such as by scanning a copyright work into digital form. Second, because the e-mail message will be saved on at least one mail server during the course of transmission, a further reproduction is made. In addition, the viewing of an e-mail message or newsgroup posting by a recipient means that another reproduction will be made at least in the RAM of the recipient's computer.

In addition, if an e-mail communication is not "to the public" so as to constitute an infringement of the exclusive right to communicate a work by telecommunication to the public, then the exception contained in the Act which provides that such communication is not a publication would not apply. Therefore, a private "e-mail communication" containing an unpublished work protected by copyright may constitute an infringing publication of the work.

5.3 Transactions involving the World Wide Web, FTP and BBSs

The nature of the World Wide Web, FTP and BBS access is different from e-mail and newsgroup postings since, even though the data must have been initially posted at the site, it is the recipient which originates and controls access to, and downloading of, the data to be retrieved. The posting of a copy of a copyright work to a Web site, FTP site or BBS will, in most cases, involve the reproduction right and the right to communicate the work to the public by telecommunication as in the case of a posting to a newsgroup.

One unique element of the Web which is critical to the issue of infringement of the reproduction right is the act of "caching". Unlike e-mail communications, the basic transmissions of the elements of a Web page from the server in which they reside to the recipient's computer is instantaneous, and need not involve a reproduction of the work by the Internet service provider ("ISP") serving the recipient. To that extent, there may be less reproductions of copyright works in Web page access than in e-mail communications. Caching, however, involves the reproduction and storage of the elements of a Web page on an intermediate server or computer so as to increase the efficiency of accessing that page. Caching is done by both ISPs and users. ISPs cache heavily-accessed pages in order to speed the access time. Caching is done sometimes "blind" by operation of the ISP's system automatically, based on demand or technical requirements, or can be done through specific choices made by the ISP for technical or commercial reasons. Caching also occurs when users access a Web page. The elements of a Web page are stored on a user's computer hard drive when a page is first accessed in a Web session and the cached copy of the Web page's elements will often be accessed later without recourse to the Internet or to a new download. In most cases, user caching will take place without any active intervention, choice or even knowledge on the part of the user. Nevertheless, because infringement of the right of reproduction does not require any knowledge, caching constitutes a reproduction and is covered by the reproduction right.

Operators of Web sites may also make unauthorized links to other Web pages. Although the copyright owner may not like the links being made by a third party to the location of its copyright works, it is difficult to see how there is any infringement of the copyright in the works to which the links point if the only thing reproduced is the title or URL address of the work. The linking Web page is no different from a footnote or bibliography which points a user to another location or source. Since, in most cases, there is no copyright in the title of a book, play or music, there likely can be no copyright in a URL address itself or in the title to which the hyperlink points.

Downloads of copyright work from Web sites, FTP sites or BBSs will involve a reproduction of those works. Most such downloads will also constitute a communication of the work to the public by telecommunication, because the nature of these sites is such that they invite a number of unrelated persons to access them in order to facilitate communications.

It is unlikely that, under Canadian law, an Internet transmission could ever be found to be a public performance. If the transmission is a communication to the public by telecommunication, then, as a result of an exception in the Act, the activity cannot also be covered by the right of public performance.

Finally, all of the prohibited acts are only infringements if they are done without the consent of the owner of the copyright. Although the Act requires that any assignment or grant of an interest in a copyright must be in writing, an implied license could be deemed to have been granted when the nature of the transaction makes it necessary to do so. The onus is on the defendant alleging the existence of an implied license to prove both the fact of the license and its operative terms. The concept of implied license is important for ISPs and other operators with respect to caching and for users with respect to browsing. If a copyright owner has permitted the work to be placed on the Internet, it could be argued that the owner has implicitly consented to caching as a necessary method of copying the work to permit the work to be accessed and transmitted to the user in an effective way. Similarly, where a copyright owner places a work on the Internet in such a way that it is freely available, it likely can be implied that any reproduction of the work necessary to permit the work to be perceived by a recipient, such as the loading of the work into the RAM of the recipient's computer, has been implicitly consented to. Such an implied license would not, however, extend to the making of a permanent copy. Although recommendation 6.4 (a) of the IHAC Report stated that "it should be left to the copyright owner to determine whether and when browsing should be permitted", the authors believe that the Canadian law of implied license already provides for a type of "browsing exemption" in the limited circumstance where the copyright owner has made the work freely available on the Internet.

5.4 Who is liable for copyright infringement?

5.4.1 Direct infringement

The Act provides that direct infringement may arise either by a person doing any of the acts which fall within the exclusive rights of the copyright owner or by a person authorizing someone else to do one of these things. Direct infringement does not require knowledge of the fact that an infringement is occurring. Innocent intention affords no defence and ignorance of the existence of copyright is no excuse for infringement. Copyright being a proprietary right, it does not avail the defendant to plead motive or intent.

Many copyright infringements may be committed on the Internet using physical equipment owned by others. By way of example, while the copy of a work could be made on the server of a BBS and retained there, it is the user posting the work on the BBS which actually makes the copy using the BBS's equipment. In these circumstances, it is relatively clear that it is the user which is infringing and not the passive equipment operator unless the operator starts being involved in the

infringing act to the point that it "authorizes" the act. The case law in Canada holds invariably that where equipment is used by a third party to infringe copyright, the owner of the equipment does not infringe so long as such owner has no control over the manner in which the primary infringer uses the equipment. The case law in Canada is that, in order to "authorize", a person must sanction, approve or countenance something more than the mere use of equipment that might possibly be used to infringe copyright. This "something more than mere use" need not go so far as to grant or purport to grant a right but it may be sufficient to establish that a person has sanctioned, approved or countenanced an infringing activity if it is shown that certain relationships existed between the alleged authorizer and the actual infringer. This concept of authorization is much different from the American concept of contributory infringement.

The narrowness of the concept of authorization is of great importance in the Internet environment since much of the infringement which occurs on the Internet will occur as a result of users giving commands which result in reproductions or communication of copyright works to the public through the use of equipment provided by others. Since it is clear that such equipment can be used, and is in fact used, for non-infringing purposes, in many cases the owner of such equipment may not be liable for the infringement.

5.4.2 Indirect infringement

Indirect infringement cannot be authorized by a third party since the acts which constitute indirect infringement are not within the list of those acts to which the copyright owner has an exclusive right. A further distinguishing feature of indirect infringement is that knowledge on the part of the infringer that copyright is being infringed, or would be infringed if the acts were done in Canada, is required. In such cases therefore, ignorance may constitute a valid defence. "Knowledge" has been interpreted to mean that information which would suggest to a reasonable man that a breach of copyright was being committed, or notice of facts such as would put a reasonable person on inquiry. Once an individual has either actual or imputed knowledge that the work dealt with may be infringing copyright, the individual has an obligation to make inquiries to ensure that the work does not infringe copyright. In the case of the intermediaries involved in the Internet content transmission chain, if the intermediary is put on notice of an infringement and takes no reasonable steps to prevent its continuation, the intermediary may be liable for indirect infringement.

Since many of the participants in the Internet content transmission chain can play various roles, it is useful to categorize the infringing activities according to such roles which can be classified in three categories: posters, recipients and intermediaries.

5.4.3 Poster

A poster places copyright content on the Internet in such a way that it can be accessed by others. Examples include sending e-mail messages, posting a message to a newsgroup, uploading a work to a server, etc. In most cases, a poster will be guilty of infringement of the reproduction right. If the poster and the recipient are both located in Canada, then, except in the case of "private" e-mail messages, a poster may also be guilty of infringement of the right to communicate the work to the public by telecommunication.

If the poster is located outside Canada, and the intended recipients are located in Canada, the better view appears to be that an infringement of the right to communicate the work to the public by telecommunication takes place in Canada. Conversely, it would appear that if a poster in Canada sends a message outside of Canada, it would not be communicating the work to the public by telecommunication in Canada, even though the message originated in Canada.

In addition, in many cases, posting a copy of an unauthorized work to a newsgroup or placing it on a BBS Web site may constitute indirect infringement under the Act if the requisite element of knowledge is present, since it could be seen to be a distribution of the work "to such an extent as to affect prejudicially the owner of the copyright" or could be a public exhibition if it is "by way of trade".

5.4.4 Recipients

It appears that in every Internet transmission, except where there is an implied license for browsing, a recipient would infringe the right of reproduction if an unauthorized copy of a copyright work is received. If the recipient is also obtaining the unauthorized work from a Web site, FTP site or BBS and is shown to be acting in collusion with the poster or the operator of such site, the recipient may also be deemed to be communicating the work to the public by telecommunication. Generally, however, the recipient of an Internet transmission is not "communicating to the public".

5.4.5 Intermediaries

Intermediaries include telecommunications common carriers, Internet service providers, operators of Bulletin Board Services (BBSs) and the like. Of all those, the telecommunications common carriers regulated by the CRTC enjoy a special situation in that their Terms of Service as approved by the CRTC provide that they are not liable for "copyright infringement arising from material transmitted or received over the carrier's facilities" or "copyright or trade-mark infringement, passing off or acts of unfair competition arising from directory advertisements furnished by a customer

or a customer's directory listing, provided such advertisements or the information contained in such listings were received in good faith in the ordinary course of business". On the other hand, other intermediaries such as Internet service providers do not enjoy this exemption or defence.

The only so-called "common carrier exemption" existing in the *Copyright Act* is a narrow exemption specifying that a person "whose only act in respect of the communication of a work to the public consists of providing the means of telecommunication necessary for another person to so communicate the work does not communicate that work to the public". This exemption only applies to infringements of the right to communicate the work to the public by telecommunications and is not an exemption with respect to other rights which could be potentially infringed, such as the right of reproduction. This exemption applies solely to the activity described in the exemption and not to any particular class or category of persons. Consequently, if all that an intermediary does in respect of an Internet transmission is provide the "means of telecommunication", then, regardless of whether or not it is a telecommunications common carrier, the intermediary will be protected by the *Copyright Act* exemption from liability for infringement of the right to communicate a work to the public by telecommunication. Conversely, even a telecommunications common carrier is not protected by this exemption in the *Copyright Act* when it infringes other rights, such as the right of reproduction.

Intermediaries may also be liable when they infringe exclusive rights directly or by authorization. As noted above, however, authorization requires more than just to provide equipment or facilities. While individual circumstances differ, in many cases intermediaries will not be liable for authorizing copyright infringements by their users.

This distinction is important since, as noted above, almost every Internet transmission involves a reproduction and a potential infringement of the reproduction right. Much of the reproduction is done on the equipment of Internet intermediaries which may cache copies of copyright works or store copies of e-mail or newsgroup messages which include copyright works. The primary determination to be made in deciding whether an intermediary will be liable for these potential infringements of the reproduction right is whether the intermediary makes a conscious decision to reproduce the work or whether it is the user which is reproducing the work using the intermediary's equipment. In the former case, the intermediary will generally be liable while in the latter case the intermediary will not be either personally infringing or authorizing the infringement by the user.

However, once the intermediary becomes aware that infringement has occurred and fails to take reasonable measures to stop the infringement, the intermediary may be guilty of indirect infringement or, in some cases, of infringement

as a joint infringer. There is an issue, as in all cases involving notice of alleged copyright infringements, of how conclusive the notice given to the intermediary must be in order to impose an obligation on the intermediary to act to try to suppress the alleged infringement. As is the case with respect to civil liability, there is a direct relationship between the level of control and knowledge which an intermediary has of a copyright infringement and an intermediary's potential liability for that infringement. It is important to note, however, that knowledge that copyright is being infringed is not in itself sufficient to impose liability for copyright infringement on an intermediary.

6. CONCLUSION

The Internet revolution poses various challenges in applying, enforcing and abiding by existing laws.

If amendments to existing laws are needed, they should only be made in a *de minimis* way and in a way as technologically neutral as possible under the circumstances. Legislators should also be mindful of the need to balance the interests of the users, publishers and disseminators on the one hand, and those of the authors, on the other, while preserving freedom of expression and only imposing limits on such freedom as necessary in a free and democratic society.

* * *

[Cat. No.: C2-312/1997E ISBN: 0-662-25489-9]

THE CYBERSPACE IS NOT A "NO LAW LAND"

A study on the issues of liability for content circulating on the Internet

"It's always surprising how old concepts carry into the new medium. It's overly idealistic to act like, Oh, the Internet is the one place where people should be able to do whatever they wish: present child pornography, do scams, libel people, steal copyrighted material. Society's values have not changed fundamentally just because it's an Internet page."

Bill Gates, Microsoft Corporation, as quoted in *George Magazine*, February 1997

1. INTRODUCTION

1.0 The Internet phenomenon

With the advent of new computer and telecommunications technology, a new world is unfolding before us. A world in which ideas can be exchanged electronically almost instantaneously around the world among millions of people using computers. A world in which expressions as varied as print, graphics, photographs, audio or video can be communicated in combinations unheard of only a scant few years ago.

This information technology revolution, like the industrial revolution, is reshaping the world and creating new paradigms in the social, cultural, economic and political domains. People located on different continents can now do research, communicate with each other and exchange goods and services without time or space barriers and with fewer intermediaries than was previously the case.

In this new world, users can become producers and producers are also users. This new world also creates realities unthinkable just a few years ago. For example, who would have thought that in order to read a document one would need to first copy it?

This new world also permits people to be able to communicate with others using their names, a pseudonym or even anonymously. It is no longer possible to verify whether the

person you are communicating with is a minor or a seventy-year old person, a male or a female.

This new world also permits any content being communicated to be reproduced, modified and re-sent to one person or to millions of persons almost instantaneously.

This new world of communications is made possible through the evolution of what is commonly known as the Internet.

The Internet started as an experimental project of the US Advanced Research Project Agency ("ARPA") and was then called ARPANET. The ARPANET was, in its origin, linking computers and networks owned by the US military, defence contractors and university laboratories conducting defence-related research. Later, ARPANET allowed researchers across the USA to access powerful super computers located in a few key universities and laboratories and later evolved to encompass universities, corporations and people around the world. The ARPANET became the "DARPA Internet" and finally the "Internet".

The Internet is not a network; it is rather an interconnection of innumerable networks of all sizes: a network of networks.

Computers and computer networks that compose the Internet are owned by governmental and public institutions, non-profit organizations, commercial organizations and individuals. The Internet is not managed at any central point.

According to figures quoted in *American Civil Liberties Union, et al.* v. *Janet Reno*[1], fewer than 300 computers were linked to the Internet in 1981, and by 1989 that number had increased to some 90,000 computers. By 1993, over a million computers were linked. Today, over 9,400,000 host computers worldwide are estimated to be linked to the Internet and this figure does not include all the computers used to access the Internet via modems. It is estimated that as many as 40,000,000 people around the world use the Internet and that figure is expected to grow to about 200 million users by 1999.

The Internet has therefore become a very powerful medium for the exchange of ideas and for the advancement of social, economic, cultural, political, scientific and personal objectives.

But, as with any such powerful "invention" (we would be tempted to describe the Internet as a "movement" rather than an invention), there comes some challenges. The Internet is a formidable tool for people to knowingly or unknowingly violate the rights of others. These violations include copyright and trade-mark infringements, attacks on the

---

[1] USDC Eastern District of Pennsylvania No. 96-963 and 96-1458, June 11, 1996, paragraph 3 of the Findings of fact.

reputation or privacy of others, communication of hate propaganda and distribution of obscene material including child pornography.

1.1 The governmental studies

Governments around the world have started to examine the issues arising from this new "information infrastructure" including whether this new era mandated any amendments to existing laws to cope with this new reality.

In February 1993, US President Clinton formed the Information Infrastructure Task Force to determine what should be the US Administration's vision for what it called the "National Information Infrastructure". A working group on intellectual property was established to examine the implications of the National Information Infrastructure and to make recommendations as to any required changes to the US intellectual property laws. This working group published its report in September 1995[2]. These issues have also been examined by the European Commission[3] and by studies in France[4], Japan[5] and Australia[6].

In Canada, the Information Highway Advisory Council ("IHAC") examined the challenges posed by this new environment and appointed a Subcommittee on Copyright to examine copyright issues raised by the information highway[7]. The IHAC adopted many recommendations relating to copyright (recommendations 6.1 to 6.16 in its final report[8]). It also addressed the issue of the liability of bulletin board system operators as follows:

> "The Council recognized that under the current law, service providers could be held liable for copyright infringement. Only common carriers that function

---

2 *Intellectual Property and the National Information Infrastructure: The Report of The Working Group on Intellectual Property Rights*, available at IITF.DOC.GOV.

3 *Copyright and Related Rights In The Information Society*, Commission Of The European Communities, Brussels, July 19, 1995, Com. (95) final.

4 *Industries culturelles et nouvelles techniques*, Ministère de la Culture et de la Francophonie, Paris, 1994, commonly known as the Sirinelli Report.

5 *A report on Discussions by the Working Group of the Subcommittee on Multi-Media Copyright Council: Study of Institutional Issues Regarding Multi-Media*, February 1995.

6 *Highways to Change: Copyright in the New Communications Environment*, Report of the Copyright Convergence Group, August 1994.

7 *Copyright and the Information Highway*, Final Report of the Subcommittee on Copyright, March 1995.

8 *Connection Community Content: The Challenge of the Information Highway*, http://info.ic.gc.ca/info-highway/ih.html.

> solely in that capacity are exempt from copyright liability under the *Copyright Act*. However, it was felt that, with the absence of any recourse to some form of defence mechanism, copyright liability of bulletin board system operators could be too rigidly interpreted." (at page 120)

The IHAC also adopted recommendation 6.16:

> "No owner or operator of bulletin board systems [BBS] should be liable for copyright infringement if:
>
> a. they did not have actual or constructive knowledge that the material infringed copyright; and
>
> b. they acted reasonably to limit potential abuses." (at page 120)

However, the IHAC report addressed only the issue of copyright liability and only that of owners or operators of bulletin board systems. In the Internet content distribution chain, more than operators and owners of BBSs are involved and more than copyright infringement is at stake. The various intermediaries include users, the Internet access providers (also called "ISP" or Internet service providers), telecommunications common carriers, BBS operators, the on-line service providers, operators and moderators of newsgroups and mailing lists, and so on.

The IHAC also recognized that: "Questions of liability of owners, operators and users need to be clarified."[9] In addition, the IHAC adopted recommendation 8.2 as follows:

> "The federal government should take immediate steps to lead in the development of legislative measures with regard to clarifying the question of liability of owners, operators and users of bulletin boards, Internet and Usenet sites." (at page 133)

Before deciding whether legislative measures were needed concerning these issues of liability, Industry Canada determined that it was best to first conduct an investigation as to what the state of the law was. It is in this context that Industry Canada commissioned Mark S. Hayes of Fasken Campbell Godfrey in Toronto, Michel Racicot of McCarthy Tétrault in Montréal, Alec Szibbo of Gowling, Strathy and Henderson in Vancouver and Pierre Trudel of the "Centre de recherche en droit public" of the Faculty of Law of the Université de Montréal, to conduct this study.

---

[9] Final report at page 132.

This substantive study is believed to be the first of its kind in the world for nowhere else has there been a study conducted on the specific issues of liability for content circulating on the Internet.

Michel Racicot was charged with overall coordination, review and critique of the study while Mark Hayes dealt with copyright issues, Pierre Trudel with civil liability issues and Alec Szibbo with trade-mark issues and issues related to the Criminal Code. However, all four authors assume full responsibility for the overall report which they have all reviewed and approved.

1.2 The Objectives

The objectives of this study are to present an analysis of the state of the law in Canada (with comparisons, where appropriate, to US and other foreign law) related to liability for content circulating on the Internet. Specific comment is made with respect to copyright, trade-mark, civil liability, privacy, and criminal law issues for Internet service providers, bulletin board services, newsgroups and other related services.

The Terms of Reference (attached as Appendix I) specifically prohibited the authors from elaborating policy options or formulating recommendations, including any legislative measures to amend existing laws. It is however hoped that the uncertainties and difficulties revealed by this study will pave the way for legislative measures aimed at clarifying the rights and obligations for users, intermediaries and authors. The Terms of Reference also excluded from the scope of the study any examination of whether any Internet services should be regulated under the *Telecommunications Act* or the *Broadcasting Act*.

The study assumes that liability is possible on the Internet. The analysis in this study is intended to help all participants in the Internet content value chain better understand their roles regarding information management liability and the effects of their activities and decisions on other stakeholders. The study is also aimed at trying to clarify the obligations of those who use and disseminate content and the rights of those who create it.

1.3 The Method

The study presents the state of the law as it existed in the fall of 1996 and does not therefore reflect the amendments to the *Copyright Act* introduced in Bill C-32, *An Act to Amend the Copyright Act*, tabled in the House of Commons on April 25, 1996, nor the two WIPO Treaties resulting from the Diplomatic Conference on Certain Copyright and Neighbouring Rights held in Geneva from December 2 to 20, 1996.

The study was made difficult by the almost complete absence of case law in Canada, especially in the areas of copyright infringement and civil liability, as compared to the US

situation where the courts have already begun to examine the copyright and civil liability issues raised by the dissemination of content over the Internet.

By way of example, the burden of proof in criminal law is much higher (beyond a reasonable doubt) that in civil law (balance of probabilities). Most offences under the Criminal Code require the presence of a guilty intent ("*mens rea*") while most infringements under the *Copyright Act* are of a strict liability nature, requiring no presence of "*mens rea*".

The study was also made difficult because the criteria for assigning liability vary greatly depending on the right or prohibition at issue. Standards under the Criminal Code, by way of example, are very different from those under the *Copyright Act* or under civil liability.

In addition, with many Internet communications involving participants in more than one country, the questions of liability related to content will necessarily involve issues of international law such as:

- which court has jurisdiction,
- is the jurisdiction determined by the object or activity ("*in rem*") or by the person ("*in personam*"),
- which conflicts of law rules should apply,
- which substantive laws should apply,
- where did the infringement take place.

These issues were beyond the scope of this study to examine exhaustively.

Although the researchers could have conducted the study by analysis of legal doctrine and case law, it was felt preferable to also obtain input from interested stakeholders. Consequently, approximately 200 invitations were sent to persons and organizations inviting their recipients to make written submissions and to participate in focus groups, which were held in Vancouver, Toronto and Montréal in the fall of 1996.

Over 20 written submissions were received[10] and the three focus groups were well attended. For reasons of confidentiality expressed at the focus group meetings, the researchers will not publish the list of attendees at the focus groups. This promise was made in order to have a more open debate in the focus groups.

Industry Canada will circulate this study in both official languages, including by publication on Industry Canada's Web site.

---

[10] See list attached as Appendix II.

It should be noted that most of the submissions provided in response to the invitations sent out by the researchers did not address in any detailed way what the state of the law is, but rather put forward either the position of the organization making the submission about its own situation or statements as to what the state of the law should be. Although this study is precluded by its Terms of Reference from making recommendations for legislative changes, we have suggested to Industry Canada that these submissions be analysed in greater detail if the Government of Canada intends to consider any legislative measures as a result of its analysis of the legal situation applicable to the Internet.

1.5 Revelations of the focus groups

The focus groups revealed that most intermediaries in the Internet distribution chain readily accept that they have some liability for the content they carry, depending on the level of knowledge and control they have in respect to that content. In this regard, the Code of Conduct issued in 1996 by the Canadian Association of Internet Service Providers (CAIP) (attached as Appendix III) is to be commended.

Content vendors have also expressed their desire to comply with the law and to accept liability for the works they make available on the Internet.

However, certain users of the Internet want to preserve the new frontier, no law, no controls, style of Internet. Since most users are also creators and since these users are also vulnerable to attacks on their privacy, reputation, morals and those of their children, we hope that this study, public debates and awareness campaigns covering the proper use of the Internet will convince them that responsible use of the Internet, like responsible use of our roads and highways, is a necessary limitation to freedom in order to live in a democratic society.

Creators, on the other hand, realize that it is the content they have created which, to a great extent, is the moving force behind the growth of the Internet and which enables intermediaries to grow and, eventually, to prosper. Creators are still waiting to see the economic benefits that the Internet can bring to them. They all hope that new systems for automatic licensing of the use of their works and other new technical avenues made possible by the Internet will bring them their fair share of the wealth so created.

What participants in the focus groups deplored is the continuing uncertainty concerning their rights, obligations and liabilities in their role as a participant in the dissemination of content on the Internet distribution chain.

It is hoped that this study will enlighten them or, at least, provide more of a focus on those issues which require clarification.

1.6 The Internet: Description and Uses

A better understanding of the liability related to content circulating on the Internet necessitates an understanding of the nature of the Internet, how it is accessed and how it is used. Rather than repeating here what others have said more eloquently or in greater detail, we refer the readers to the findings of facts reproduced as paragraphs 1 to 48 in *American Civil Liberties* v. *Reno*[11], which the researchers have found represents one of the best descriptions from a layperson's perspective. There are also innumerable treaties and articles published on the subject, some of which are referred to in footnotes throughout the study. As will be found in these descriptions, various actors (users, Internet service providers, telecommunications common carriers, on-line service providers, etc.) participate in the distribution of content on the Internet in various ways. Therefore, it cannot be emphasized enough that it is not the status of an "actor" that is important in the determination of liability, but rather the specific activity performed by such an "actor".

By way of example, the so-called "common carrier exemption" contained in paragraph 3(1.3) of the *Copyright Act* (R.S.C. 1985, c. C-42, as amended) does not *per se* apply to a telecommunications common carrier (as understood in the *Telecommunications Act*, S.C. 1993, c.38, as amended) but attaches rather to a certain activity (only "providing the means of telecommunication necessary for another person" to communicate a work to the public). At times, a telecommunications common carrier can become a publisher (for example, when it puts content on its own Web site). Conversely, an on-line service provider whose main activity may be that of publishing may at times have activities analogous to that of a telecommunications common carrier, for example when it only provides means of telecommunication necessary to have access to the Internet. In this regard, generalities must be avoided.

1.7 A word of caution

A word of caution before reading further must be made. When discussing these types of issues, one is naturally drawn to US precedents in light of the abundance of US case law which has caused many emerging issues to be examined first in the US. However, it must be emphasized that although resorting to the US authorities is useful, the analysis done by US authors and US courts cannot be imported into analysing the laws of other countries, including Canada, without the necessary distinctions being made[12] even if the United States authorities have been relied upon for assistance and have been given qualified approval in

---

[11] Available on the Internet at the following address: http:\\www.aclu.org\court\cdadec.html.

[12] See in particular the comments of Estey J. in *Compo Co. Ltd.* vs. *Bluecrest Music*, [1981] 1 S.C.R. 357.

many Canadian cases[13]. While this problem has been identified in the past in respect of *Copyright Act* issues, it applies with even greater force in matters relating to civil liability (where Québec in particular has the Québec Civil Code), to privacy issues and to those issues addressed in the Criminal Code of Canada (such as hate propaganda, obscenity and child pornography).

Even within a single country, differences in provincial or state laws or different community standards must also be considered. For example, in *Thomas* v. *United States*[14], a California computer Bulletin Board System operator was convicted in Tennessee of transmitting obscene images to subscribers who downloaded them using personal computers and modems. The accused claimed that if the more relaxed community standards of California rather than those of Tennessee had been applied, he would have been found not guilty. All these distinctions must not be forgotten, although the authors have not repeated them throughout the study.

* * *

[Cat. No.: C2-312/1997E ISBN: 0-662-25489-9]

---

13 See, for instance, *Corp*. v. *Ordinateurs Spirales Inc.* (1984), 2 C.I.P.R. 56 (Fed. T.D.); *La Société d'informatique R.D.G. Inc*. v. *Dynabec Ltée* (1984), 6 C.P.R. (3d) 299 (Que. S.C.); *Apple Computer Inc*. v. *Mackintosh Computers Ltd.* (1986), 28 D.L.R. (4th) 178 (Fed. T.D.), varied (1987), 44 D.L.R. (4th) 74 (Fed. C.A.), affirmed [1990] 2 S.C.R. 209; *Delrina Corp*. v. *Triolet Systems Inc.* (1993), 47 C.P.R. (3d) 1 (Ont. Gen. Div.); *Matrox Electronic Systems Ltd*. v. *Gaudreau*, [1993] R.J.Q. 2449 (C.S.); *Prism Hospital Software Inc*. v. *Hospital Medical Records Institute* (1994), 57 C.P.R. (3d) 129 (B.C.S.C.).

14 No. 95-1992, Certiorari denied October 7, 1996; see *Computer and On-line Industry Litigation Reporter*, November 5, 1996, page 23-189.

OBSCENITY

I. PROHIBITED CONDUCT

1.Overview of Applicable Law on Obscenity

General

Obscenity is defined in the Canadian Criminal Code as any publication whose dominant characteristic is the undue exploitation of sex, or of sex together with crime, horror, cruelty or violence.[1] Whether a publication's dominant theme is the undue exploitation of sex is determined by reference to a "community standards test"[2] and an examination of the alleged obscenity within the context of the work as a whole.[3]

Subsections 163 (1) and (2) of the Act create two distinct offences. First, Subsection (1) targets the *production or distribution* of obscenity. It applies to everyone who "makes, prints, publishes, distributes, circulates", or has in one's possession for the purpose of distribution, obscene materials. Subsection (1) has been held to be a strict liability offence. Once the Crown proves illegal act of the offense, the burden falls upon the accused to avoid liability by showing that he acted with due diligence. In other words, lack of knowledge that the material exceeded community standards will not be a defense, unless the accused can establish due diligence, a reasonable mistake of fact [4] or that the public good was served.[5]

---

[1] *Criminal Code*, s. 163(8).

[2] The community standards test considers what the community would tolerate others being exposed to on the basis of the degree of harm that may flow from such exposure. The stronger the risk of harm, the less the likelihood of tolerance. For the purposes of the community standards test, the Supreme Court of Canada referred to three categories of sex: (1) sex with violence; (2) explicit sex which subjects people to treatment that is degrading or dehumanizing; and (3) explicit sex without violence that is neither degrading nor dehumanizing. The first category will almost always constitute the undue exploitation of sex. The second category may be undue if the risk of harm is substantial. The third category will generally not fall within the definition of obscenity unless it employs children in its production: *R v. Butler* (1992) 70 C.C.C. (3d) 129, 11 C.R. (4th) 137 (S.C.C.)

[3] Upon determining that the material involves the undue exploitation of sex, the portrayal of sex is then viewed in context to determine whether it is the dominant theme of the work as a whole or whether it essential to a wider artistic, literary or other similar purpose and therefore falls within the "public good" exemption: *Butler*, ibid.

[4] *R. v. Metro News Ltd*. (1986) 20 C.C.C. (3d) 35 (Ont. C.A.)

[5] *Criminal Code*, s. 163(3)

On the other hand, subsection (2) makes it an offence to *knowingly sell or expose to public view*, or to have in possession for the purposes of selling or exposing to public view, obscene materials. Unlike the distribution section, a charge under subsection (2) requires the Crown to prove that the accused had a subjective knowledge of the content and nature of the obscene material in question.[6]

"Distributor" versus "Retailer"

Cases that have considered the difference between subsections 163(1) and (2) have held that something more than offering obscene materials by one or more individual sales is required for a charge under subsection (1).[7] Thus, a video store outlet that merely rents videos is characterized as a retailer under subsection (2).[8] As a retailer, it is not involved in distribution and is therefore not required to know the contents of every video, book or magazine in its store, since imposing such a requirement would impose an undue burden on the retailer.[9] On the other hand, a video store that also creates or copies the videos on premises would be deemed to be a distributor, and for purposes of section 163(1) would *not* require proof that it had knowledge of the obscene materials.[10]

The courts have also characterized the distinction between production and distribution of obscene materials on the one hand section 163(1) and selling or exposing to public view on the other (s.163(2)), by noting that the latter is intended to cover activities in which the accused deals only with the ultimate consumer.[11] This distinction seems to have been rejected by a British Columbia Provincial Court as not necessarily being applicable to the supply of materials by computer technology.[12]

---

[6] . *R. v. Jorgensen* (1995) 102 C.C.C. (3d) 97 (S.C.C.).

[7] *R. v. Dorosz* (1971) 4 C.C.C. (2d) 203 (Ont. C.A.); *R. v. Householder T.V. and Appliances Ltd.* (1985) 20 C.C.C. (3d) 571 (Ont. C.A.).

[8] *Householder*, ibid.

[9] *Jorgensen*, supra note 6.

[10] *R. v. Harris* (1987) 35 C.C.C. (3d) 1 (Ont. C.A.).

[11] *Dorosz*, supra note 7.

[12] *R. v. Hurtubise*, Unreported, June 28, 1996, B.C. Prov. Ct., Surrey Registry.

2.Application to Internet Resources

To date, there have only been two decided Canadian cases that have considered the obscenity provisions in the context of online communications.[13] A third case is pending before the British Columbia Provincial Court, with the decision due to be released in the fall of 1996.[14]

In *Pecciarich*, a BBS co-system operator was charged under both the obscenity and child pornography provisions for uploading files to the bulletin board. *Hurtubise* and *Clark* are similar cases in which the operators of "adult" BBSs were charged with both obscenity and child pornography in the content supplied for access by their subscribers. As all three cases deal only with computer bulletin boards, their application to other Internet activities remains uncertain. However, they offer a valuable starting point, as discussed below, in analyzing this area.

"Distribution"

Both *Hurtubise* and *Pecciarich* suggest that a BBS can be held to be a distributor for the purposes of subsection 163(1). The decision in *Hurtubise*, however, is being appealed, partially on the basis that the trial judge erred in classifying a BBS as a distributor rather than a retailer.[15] Both decisions being only at the Provincial Court level are not binding on the higher courts.

Although the video store distributor-retailer analogy may seem appropriate for the various participants in the Internet context, it was rejected as inapplicable to a computer bulletin board by the court in *Hurtubise*. The court applied a broad dictionary definition of distribution, that included "to deal out, give a share of each of a number, spread about, scatter, put at different points, divide into parts, arrange, classify", and concluded that the BBS clearly fell within this definition. The court appears to have been influenced by several factors, in particular the number of people who could access the service, the potential for the information to exponentially spread to further parties, and the ability to make tangible copies of the illegal material.

> "By making a CD accessible through a local computer bulletin board, the contents of the CD become readily accessible to multiple computers. Around each computer, there would be multiple users. The contents of

---

[13] *R. v. Pecciarich* (1995) 22 O.R. (3d) 748 (Ont. Prov. Ct.); and *Hurtubise*, ibid, on appeal to be heard December, 1996.

[14] *R. v. Clark*, B.C. Prov. Ct.

[15] Comments from Crown counsel Peter Gulbranson, who prosecuted both the *Clark* and *Hurtubise* cases.

> each file on the CD can of course, be downloaded, kept on the computer, copied to another disk, uploaded to other systems, or put into hard print. This is not, in my view, analogous to an individual retailer who is selling individual copies, even if multiple copies, of books or movie video cassettes."[16]

As these factors appear equally applicable to newsgroups, Web sites and possibly mailing lists, a court could conceivably hold that supplying information through these applications also constitutes "distribution" for purposes of section 163(1).

The other notable comment on distribution in the context of a BBS is the court's holding in *Pecciarich* that "... evidence of the uploading of the files onto bulletin boards, which the public can access through an application process, is clear evidence of distribution."[17] The reference to "application process" appears to make this ruling narrower than that in *Hurtubise*, and leaves its applicability to newsgroups or Web sites that have no similar application process unclear. However, the application process did not appear to be a significant factor in the decision, and may be interpreted by subsequent courts as being immaterial.

"Publication"

On the issue of publication, the court in *Hurtubise* looked to a broad dictionary definition that included "making publicly known; issuing of book, engraving, music, etc., to the public." The court concluded that the defendants possessed the obscene material for the purpose of publication "... because of the capabilities of the computer to show material to a number of parties and to produce material easily and inexpensively ..."[18] The ability of other computer applications to provide easy, inexpensive access to large numbers of people suggests that information supplied by newsgroups, mailing lists and Web sites may also be similarly held to be publication.

"Exposing to Public View"

"Exposing to public view" is only an offence under section 163(2) when the group exposed to the obscene material is *public*. It is not an offence to expose obscene material to *private* view. For example, showing obscene material to a few friends

---

[16] *Hurtubise*, supra note 12.

[17] *Pecciarich*, supra note 13.

[18] *Hurtubise*, supra note 12.

in the privacy of one's home is not "exposing to public view.[19] Showing an obscene film to a group of 25 invited friends at a stag party is also not exposing to public view.[20] On the other hand, where the invitation goes beyond invitees to a private function and includes admission to others upon payment of a fee, the act of exposing to public view occurs.[21]

The court in *Hurtubise* noted that "computer technology permits access and the viewing of obscenity and child pornography in a variety of ways." Whether a transmission over a computer system "exposes to public view" for the purposes of subsection 163(2) will be a question of fact, dependent on the circumstances of each case.[22] The court was satisfied that providing information through a local BBS in this case constituted "exposing to public view" notwithstanding the efforts made to limit access to adult users. Because each case must be assessed on its own facts, *Hurtubise* does not necessarily preclude the possibility of a BBS in other circumstances being characterized as "private". With respect to other applications, the broad references in the case to "computer technology" may suggest that supplying information through newsgroups, and open mailing lists and Web sites would also be held to constitute "exposing to public view". It is unclear whether a court would view posting to a closed mailing list only as exposing to *private* view. *Harrison* and *Rioux* appear to suggest that a mailing list of a small number of people where the subscribers are invited to join but are not required to pay fees for the privilege might be held to be private.[23]

Intentional Causation/Due Diligence

An accused charged with publication or distribution under subsection 163(1) could avoid liability by showing that it did not intentionally cause the prohibited activities and exercised due diligence .[24] Due diligence means taking reasonable care in the circumstances (i.e. not being negligent). Though the court in *Hurtubise* found that the accused did not exercise due diligence, its comments on what the defendants could have done indicates the kinds of factors a court will consider when assessing whether due diligence was present:

---

[19] *R. v. Rioux* [1970] 3 C.C.C. 149 (S.C.C.).

[20] *R. v. Harrison* (1973) 12 C.C.C. (2d) 26 (Alta. Dist. Ct.).

[21] *R. v. Vigue* (1974) 13 C.C.C. (2d) 38 (B.C. Prov. Ct.).

[22] *Hurtubise*, supra note 12.

[23] *Harrison*, supra note 20, and *Rioux* supra note 19.

[24] *R. v. Metro News Ltd.*, supra note 4.

> "Although they made efforts to ascertain how they could restrict access to adult users, they made no effective inquiries as to content. They did not obtain any advice as to the meaning of "obscenity" and did not distinguish between pornography and obscenity. They did, however, clearly recognize that some of the material which people were transmitting was offensive ... Even after being alerted to this kind of material they made no effort whatsoever to review the material on [their own] CD. They did not review the file names in the directories, any sampling of the material on the CD, nor even look at what was contained on the CD."[25]

[25] *Hurtubise*, note 12.

II. ACTIVITIES AT RISK

1.Access Provider's Facilities Used to Transmit Obscene Materials by its Users

Issue

An access provider that merely provides users with a connection to the Internet could potentially be liable for the obscene materials transmitted by its users.

Party Potentially Liable

The access provider could be charged with distribution under subsection 163(1) for its role in facilitating access to the illegal materials. Distribution of obscenity is a strict liability offence. Once the Crown establishes that the provider facilitated the transmission of the obscene materials, the provider will need to show that it exercised reasonable care in preventing obscene materials from being transmitted through its system. This may be difficult for an access provider to do, as most providers are akin to common carriers, in that their transmitting services are not affected by or subject to the content of the transmission.

An access provider could attempt to challenge the characterization of providers as "distributors" by relying on the Supreme Court of Canada's decision in *Jorgensen*.[26] *Jorgensen* noted that while producers and distributors are presumed to be familiar with their material by virtue of creating or distributing it, "... it would be perfectly reasonable to assume that the seller would ordinarily not be aware of the specific nature of the contents of the material sold" due to the vast number and variety of the books, magazines or videos in the retail outlet. *Jorgensen* further stated that knowledge of the specific nature of the contents could not be assumed with films, videos *and other media* involving a collection of images where it takes *time and active steps* to observe and 'know' the contents. For these reasons, the court concludes that imposing a burden on a seller to be familiar with the content of each book or video in order to sift out illegal materials would impose an unreasonable burden on the retailer.

The provider could try to portray itself in the same category as a book or video store vendor, by drawing attention to two similar factors. First, the sheer volume of material transmitted by its server makes it impossible for it to know the contents of each file or message sent by its customers. Second, even if it wanted to view the contents of the files or messages, doing so would require what *Jorgensen* refers to

[26] *Jorgensen*, supra note 6.

as "time and active steps". Just as it would be unreasonable to expect a video store owner to view every video, so too it would be unreasonable to expect an access provider to view the contents of every transmission. In fact, the argument in *Jorgensen*'s appears to apply even more strongly for an Internet access provider than a video retailer, since each video's physical delivery to the store virtually guarantees that the retailer will at least be aware of its existence before putting it out for sale. In contrast, a provider will probably not be aware of an offensive transmission until it is brought to its attention by either taking the "time and active steps", or some other extraordinary means.[27]

The Crown would of course rely on *Hurtubise*, which held that a BBS was clearly a distributor. That decision could be distinguished on two points. One of the BBS operator's central roles is to supply content to its subscribers; the access provider merely facilitates transmissions. In addition, the BBS operator has the means for both knowledge and control - it can relatively easily examine the content to ensure that it is not obscene. On the other hand, access providers are not privy to their subscribers, content either in detail or even generally, nor do they readily have control over what their subscribers access or send.

If the court accepts the argument that the more appropriate charge would be "selling or exposing to public view" (subsection 163(2)) rather than "distributing" (subsection 163(1)), then the Crown would have to prove that the provider had a subjective knowledge of the presence and nature of the obscene materials in question.[28] The provider would in this instance also attempt to rely on *Jorgensen* to suggest that it could not be expected to know the contents of each of its transmissions.

Relevant Legislation

Subsections 163(1) and 163(2) of the *Criminal Code*.

Relevant Case Law

R. v. Jorgensen [1995] 4 S.C.R. 55;
R. v. Hurtubise, Unreported, June 28, 1996, Surrey Registry, B.C. Prov. Ct.

---

[27] For example, the access provider could be alerted to the illegal material by other users.

[28] *Jorgensen*, supra note 6; *R. v. Metro News Ltd.*; supra note 4.

Self-Aide Practises

The access provider could minimize its risks by:

(i) obtaining a legal opinion on and understanding the distinction between pornography and obscenity;[29]

(ii) implementing an "Acceptable Use Policy" that clearly forbids users to transmit obscene material;

(iii) reviewing any material if brought to its attention; and

(iv) establishing a policy for dealing with users found to be transmitting such illegal materials.[30]

Such steps may help the provider establish a due diligence defense to a charge of publication or distribution under subsection 163(1).

2.Obscene materials supplied by information provider

Issue

An information provider may itself supply content as part of its services, making it available through its bulletin board, newsgroup, Web site or online service. The information provider may or may not know that the content contains obscenity that is illegal. Operators of adult BBSs, in particular, may supply what appears to be legal pornography, without realizing that some of the material is actually obscene. This oversight can be due to either a lack of understanding of the distinction between legal pornography and obscenity, or a failure to adequately screen the materials.

---

[29] Note that even an honest and reasonable belief by the information provider, or even its lawyer, that material is *not* obscene will not necessarily protect the provider from liability, since whether or not material is obscene is a question of law to be determined by the court: *R. v. Regina News Ltd.* (1987), 39 C.C.C. (3d) 170 (Sask. C.A.); *Metro News*, supra note 4. In other words, if a court finds that the material in question is obscene, the provider may be liable notwithstanding its belief to the contrary.

[30] For example, the responses could range from issuing a warning, to suspending the users' privileges, to terminating their account.

Parties Potentially Liable

(i) Information Provider:

Evidence that the information provider uploaded the materials will be evidence of distribution.[31] In such a case the information provider may be liable for publishing or distributing under subsection 163(1), even if it was not aware of the existence of the obscene materials.[32] In defense to a charge under subsection 163(1), the provider will have to show that it acted with due diligence, as discussed above.

If the information provider expressly knew of the content and nature of the obscene materials, it could also be liable for selling or exposing obscene materials to public view under subsection 163(2).[33]

(ii) Access Provider:

If the information provider uses a separate access provider for its connection to the Internet, the access provider may be liable for distribution of obscene materials under section 163(1), as discussed above.

Relevant Legislation

Subsections 163(1) and 163(2) of the *Criminal Code*

Relevant Case Law

R. v. Pecciarich (1995) 22 O.R. (3d) 748 (Ont. Prov. Ct.)
R. v. Hurtubise, Unreported, June 28, 1996, Surrey Registry, B.C. Prov. Ct.

Self-aide Practices

Self-aide practices will obviously not help the provider who deliberately supplies obscene materials with the knowledge that they are illegal .

The information provider who unwittingly posts obscenity with the intent of supplying only legal materials could minimize its risk of being found guilty by:

---

[31] *Pecciarich*, supra note 13.

[32] *Hurtubise*, supra note 12.

[33] Ibid.

(i) educating itself on the difference between pornography and obscenity;[34]

(ii) adopting a procedure for screening its content (for example, reviewing file names, carefully screening *individual* files before posting);

(iii) upon becoming aware that particular materials are potentially obscene, the information provider should immediately assess the content and delete any illegal materials from its system and post a notice to all subscribers regarding the incident and the action taken;

(iv) encoding potentially offensive content so that users seeking to view the contents are forced to take affirmative steps (such as decoding) in order to view the material; and

(v) requiring a password to access the "adult" portions of the BBS, newsgroup, Web site or online service.

Such actions may help the information provider establish a due diligence defense to a charge of distribution or publication under subsection 163(1).

3.Obscene Materials Posted to Newsgroup or BBS By Subscriber

Issue

A subscriber posts content containing obscenity to a newsgroup or a bulletin board.

Parties Potentially Liable

For the purposes of discussing the liability of each of the following parties, posting material to a newsgroup or bulletin board will be assumed to constitute publication or distribution of obscene materials under subsection 163(1) or exposing it to public view under subsection 163(2).[35]

---

[34] But even an honest and reasonable belief by the information provider, that material is not obscene, will not protect the provider from liability: *Regina. News Ltd.*, supra note 29; *Metro News*, supra note 4.

[35] See *Hurtubise*, supra note 12.

(i) Subscriber:

While the only authority dealing with "distribution", "publication" and "exposing to public view" in an online context considered a BBS rather than a newsgroup, there do not appear to be any significant distinguishing features that would make a posting to a newsgroup any less of a "publication", "distribution" or "exposing to public view" than one to a BBS. Thus, the subscriber who posted the obscene material will likely be liable for publication or distribution under subsection 163(1), or for exposing to public view under subsection 163(2), provided the subscriber is located in Canada and is readily identifiable.[36] Since the act of posting suggests, at least in the first instance, that the subscriber was aware of the nature and content of the material, it may be difficult to establish a due diligence or lack of knowledge defense, although this will depend on the particular facts of the case.

In addition, if the subscriber retained a copy of the obscenity on its hard drive, printed it or saved it to disk, the subscriber may be liable for possession for the purpose of publication or distribution under subsection 163(1).

(ii) Newsgroup or BBS Operator:

The liability of an operator for the content posted to its newsgroup or bulletin board may depend to some degree on whether the operator is located in Canada and whether the newsgroup is moderated or unmoderated. If the operator is located in Canada, and the material is made available to any Canadian subscribers (which in most cases will be the situation), then the *Criminal Code* would most likely apply.

(1) Moderated Newsgroup/BBS:

Although there have not yet been any cases on this point, a court may hold that a newsgroup operator who uses a submission moderator to review subscribers' postings, either knew or should have known that the postings contained obscenity. The operator's failure to remove or otherwise deal with the illegal materials could be seen as indicating a lack of due diligence and could thus make it liable for distribution or publication under subsection 163(1). On the other hand, the due diligence standard only demands that reasonable efforts be made. The court may be prepared to recognize that despite an operator's efforts to prevent illegal

[36] Subscribers may not be readily identifiable if they posted the material through a source difficult to trace such as an anonymous remailler.

postings, obscene materials will occasionally escape detection. It may hold that, on this basis, the operator should not be liable if it otherwise exercised due diligence.

If the operator knew, whether through the moderator or otherwise, of the content and nature of the obscene materials, it could be held to be liable for selling[37] or exposing them to public view, under subsection 163(2) particularly if it took no steps to terminate such activities.[38]

***(2) Unmoderated Newsgroup/BBS*:**

The operator of an unmoderated newsgroup may also be liable for publication and distribution under subsection 163(1) on the basis that failure to appoint a moderator did not meet the standard of due diligence, due to the potential for illegal activities to occur. Liability for exposing obscenity to public view, under subsection 163(2), would likely arise only if it had had knowledge or reason to believe that obscenity was being posted to its newsgroup.

(iii) Submission Moderator:

Although there have not yet been any cases dealing with this issue, a submission moderator may be held liable for publication or distribution of obscene material, under subsection 163(1), or for exposing it to public view under subsection 163(2), on the basis that the moderator's role of accessing and reviewing postings provides the moderator with the specific knowledge and the ability to delete or permit the content to be posted. Furthermore, if the moderator fails to exercise reasonable care in reviewing the submitted material, he could be held to not be exercising "due diligence" under subsection 163(1).

(iv) Access Providers:

The reference made here is to Internet newsgroups in general, ("Usenet") rather than newsgroups confined to the subscribers of a particular BBS or online service. The international nature of Usenet newsgroups makes it virtually impossible for any one site to exercise editorial control over the

[37] The act of selling would likely be satisfied if the operator charges fees for either material downloaded or membership privileges.

[38] *Hurtubise*, supra note 12.

postings by the newsgroup's subscribers.[39] The Internet provider's control is thus limited to either offering or blocking access to a particular newsgroup.

Although there have not yet been any cases dealing with this point, an access provider's decision to provide to a Canadian resident access to a particular newsgroup could be deemed to be an affirmative act sufficient to constitute distribution under subsection 163(1). The access provider could challenge the characterization of a provider as a distributor, by relying on *Jorgensen* to describe itself as a "retailer" with no responsibility for all of its products, as per the discussion above. If the Crown succeeds in establishing distribution, the onus will shift to the access provider. The access provider's failure to block the newsgroup carrying obscene materials may be seen as indicating a lack of due diligence. This is particularly the case if the newsgroup's history or character provides the access provider with reason to believe that the newsgroup may contain potentially illegal materials (such as those in the *alt.sex.binaries* hierarchy) and fails to reasonably investigate the content, or the access provider becomes aware of the nature and content of the obscenity posted to the newsgroup, but fails to block access to the newsgroup subsequent to the discovery.

The provider may also become liable for exposing obscenity to public view under subsection 163(2). The provider could try to raise *Jorgensen* as a defense to suggest that it, like the video store owner, cannot be expected to be familiar with the contents of each posting to newsgroups that it carries, due to the vast number of postings and the time and active steps that would be needed to view the materials.[40] Such a defence would of course not assist it, if the provider became aware of any specific obscene material and failed to act.

(v) Universities as Access Providers:

Although universities are only a subcategory of access providers, they possess unique characteristics that require examination of their liability within a separate context. In a speech given to a free speech symposium in 1994, Mr. Justice Sopinka of the Supreme Court of Canada noted that attempts to block access to certain newsgroups would be viewed as censorship, and issues of censorship are particularly sensitive where institutions of higher learning are involved. Although there have not yet been any cases dealing with whether a university's failure to block access

[39] This is not to say that there is no operator administering the Usenet newsgroup. However, the operator is not necessarily resident in Canada and may or may not be known to the access provider.

[40] *Jorgensen*, supra note 6.

to an offending newsgroup constitutes a lack of due diligence for purposes of subsection 163(1), Mr. Justice Sopinka's comments offer an insight into how the courts might address the issue. He noted that a university which blocks access to newsgroups risks being characterized as a government actor for the purposes of the *Canadian Charter* and having its activities scrutinized as a breach of the *Charter*'s guarantee of freedom of expression.[41] He suggested that before taking action to ban offensive communications, a university should consider whether it is not preferable to limit the expression and allow the criminal or civil law to deal with the individual who publishes the material rather than to prevent the speech before it can be expressed. These comments suggest that a university's decision to continue offering access to a newsgroup with "illegal" content may not necessarily be seen as a lack of due diligence for the purpose of subsection 163(1).

Relevant Legislation

Subsections 163(1) and (2) of the *Criminal Code*
Section 2(b) of the *Canadian Charter of Rights and Freedoms.*

Relevant Case Law

R. v. Jorgensen [1995] 4 S.C.R. 55

Self-aide Practices

(i) Subscriber:

The subscriber who posts materials could minimize its risk by:

(1) educating itself on the difference between pornography and obscenity;[42] and

(2) reasonably screening the contents of any materials prior to posting.

---

[41] Canadian Charter of Rights and Freedoms, section 2(b). The policy conflict between free speech and censorship in the guise of legitimate control over indecent and obscene materials was recently reviewed by several United States Courts when the constitutionality of the*U.S. Communications Decency Act of 1996* was challenged: *ACLU v. Reno,* 1996 U.S. Dist. Lexis 7919 (E.D. Pa. 1996); *Shea v. Reno,* 1996 U.S. Dist. Lexis 10720 (S.D.N.Y. July 29, 1996)

[42] Not a complete defence; *Regina News Ltd.*, supra note 29; *Metro News*, supra note 4.

(ii) Newsgroup Operator / BBS Operator / Submission Moderator/ Access Provider

A newsgroup operator, BBS operator, submission moderator or access provider could minimize its risk of liability by undertaking a number of the following activities:[43]

(i) educating itself on the difference between pornography and obscenity;[44]

(ii) adopting and implementing a procedure for screening online content (for example, reviewing file names, carefully screening *individual* files before posting);

(iii) adopting an "Acceptable Use Policy" that: (a) expressly forbids the exchange of obscenity or other illegal materials; and (b) requires its users to immediately notify the information provider of any illegal materials found on the system; and

(iv) adopting a procedure for responding to illegal materials: upon becoming aware that particular materials are potentially obscene, the provider should immediately assess the content, delete any illegal materials from its system and post a notice to all subscribers regarding the incident and the action taken;

(v) posting warnings of potentially offensive content;

(vi) encoding potentially offensive content so that users seeking to view the contents are forced to take affirmative steps (such as decoding) in order to view the material; and

(vii) requiring a password to access the "adult" portions of the BBS, or newsgroup.

Such steps may help the parties establish the due diligence defense to a charge of publication or distribution under subsection 163(1).

---

[43] Some of the suggestions, such as the ones in (ii) and (iv), will be more appropriate for the newsgroup or BBS operator than for the access provider.

[44] See note 42.

4. Obscene Materials Transmitted Through Mailing List

Issue

A subscriber in Canada transmits content containing obscenity directly to other mailing list subscribers.

Parties Potentially Liable

For the purposes of discussing the liability of each of the following parties, posting material to a mailing list will be assumed to constitute publication or distribution of obscene materials under subsection 163(1) or exposing obscene materials to public view under subsection 163(2).[45]

(i) Subscriber:

The subscriber's liability for publication, distribution, possession of obscenity for the purpose of distribution and exposing it to public view will likely be similar to the liability of a subscriber who posts obscene material to a newsgroup or BBS, as discussed above.

(ii) Mailing List Operator:

The liability of the operator may depend to some degree on whether the mailing list operator is located in Canada and whether the mailing list is open or closed and moderated or unmoderated.

***(1) Open Mailing List - Moderated*:**

The liability of an operator of a moderated open mailing list will likely be similar to that of a moderated newsgroup operator, as discussed above.

***(2) Open Mailing List - Unmoderated*:**

The liability of an operator of an unmoderated open mailing list will likely be similar to that of an unmoderated newsgroup operator as discussed above.

---

[45] See *Hurtubise*, supra note 12.

(3) Closed Mailing List:

The liability of a closed mailing list operator may depend on whether the mailing list is considered a "private medium".[46]

In response to a charge of distribution or publication under subsection 163(1), the operator could seek to distinguish the mailing list from other modes of distribution or publication by stressing that a mailing list is a "private communication" which lacks the essential "public" element. In cases dealing with the interception of private communications, the courts have held that whether a communication can be considered private depends on the user's expectation of privacy with respect to that communication. On this basis, telephone calls have been held to be private,[47] while pager messages pager and messages left at a computer message center have not.[48] The courts may be reluctant to characterize a mailing list as a private communication due to the potential many-to-many nature of the communication and a subscriber's inability to control what other subscribers do with the message once it is posted. The message, once sent, could be easily downloaded, printed or forwarded to another person; in each case, the message may be readily viewed by people other than the subscribers. For these reasons, a high expectation of privacy in a mailing list may be considered unreasonable.

If the court refuses to characterize the mailing list messages as private communications, a provider charged under subsection 163(1) will have to establish that it acted with due diligence to avoid liability.

Alternatively, if the operator knew of the content and nature of the obscene materials, and took no action in response, it could be liable for exposing obscenity to public view under subsection 163(2). The operator could attempt to defend by suggesting that the mailing exposes the material to *private* rather than *public* view. In the stag party examples, the courts distinguished between a small number of invitees, which was deemed private,[49] and a larger

---

[46] See the corresponding discussion of e-mail as a "private communication" in section (II)(5)(B)(i), below.

[47] *R. v. Monachan* (1981), 60 C.C.C. (2d) 286 (Ont. C.A.), affd 16 C.C.C. (3d) 576 (S.C.C.).

[48] *R. v. Lubovac* (1989), 52 C.C.C. (3d) 551 (Alta. C.A.).

[49] *Harrison*, supra note 20.

number of invitees plus paying guests.[50] It is conceivable that obscene material posted to a small mailing list would not constitute an offence if the subscribers neither paid for the materials nor membership privileges. It is unclear, however, where the court would draw the line with respect to the number of subscribers or type of membership limitations and terms.

(iii) Submission Moderator:

The liability of the mailing list's submission moderator will likely be similar to that of a newsgroup's submission moderator, as discussed above.

(iv) Access Provider:

The access provider could be potentially liable for distribution under subsection 163(1) for its facilitating access to the obscene material on the mailing list. See the discussion of access provider liability for distribution above.

Relevant Legislation

Subsections 163(1) and (2) of the *Criminal Code.*

Relevant Case Law

Beaver v. The Queen (1957) 118 C.C.C. 129
R. v. Harrison (1973) 12 C.C.C. (2d) 26 (Alta. Dist. Ct.)
R. v. Vigue (1974) 13 C.C.C. (2d) 38 (B.C. Prov. Ct.)

Self-aide Practices

(i) Subscriber:

The subscriber could minimize its risk by:

(1) educating itself on the difference between pornography and obscenity;[51] and

(2) undertaking a screening program of the contents of any materials to be posted to the mailing list prior to posting.

---

[50] *Vigue*, supra note 21.

[51] Only a partial answer: *Regina News Ltd.*, supra note 29; *Metro News*, supra note 4.

(ii) Mailing List Operator / Submission Moderator / Access Provider:

The mailing list operator, submission moderator and access provider could minimize their risk of liability by:[52]

(i) each educating itself on the difference between pornography and obscenity;[53]

(ii) adopting and implementing a procedure for screening online content

(iii) adopting an "Acceptable Use Policy" to forbid the exchange of obscenity and require users to immediately notify the information provider of any illegal materials;

(iv) upon becoming aware that particular materials are potentially obscene, assess the content and delete any illegal materials from its system and post a notice to all subscribers regarding the incident and the action taken;

(v) posting warnings of potentially offensive content;

(vi) encoding potentially offensive content; and

(vii) requiring a password to access the mailing list messages.

Such steps may help the parties establish the due diligence defense under subsection 163(1).

5. Obscene Materials Transmitted Through E-Mail

Issue

A subscriber in Canada transmits content containing obscenity to a select few (one or more) persons through e-mail. The obscene materials may be in either the message itself, or in an attached file.

---

[52] Some of the suggestions, may be more appropriate for the mailing list operator than for the access provider.

[53] See note 51.

Parties Potentially Liable

(i) Subscriber:

The liability of the subscriber may depend on whether e-mail is considered a private medium.

The subscriber may escape liability for publication or distribution under subsection 163(1), or for exposing to public view under subsection 163(2) if the court finds that e-mail is a "private communication". There have not yet been any cases that have considered the nature of an e-mail communication. While *Hurtubise* made a reference to e-mail as being a private communication, this reference was made only in passing. Cases dealing with the interception of private communications have held that whether a communication can be considered private depends on the user's expectation of privacy with respect to that communication. On this basis, telephone calls have been held to be private,[54] while pager messages and messages left at a computer message center were not.[55]

While Canadian courts have not yet considered the nature of e-mail, the U.S. Military Court of Appeal has considered the privacy issue of e-mail during an appeal from a conviction for distributing child pornography through e-mail.[56] Though the issue involved whether the search of the defendant's e-mail messages violated his Fourth Amendment rights, the analysis of principles applied by the court is somewhat similar to that in Canadian cases dealing with the interception of private communications. The court applied a two-pronged test to determine whether the accused had an actual (subjective) expectation of privacy and whether the accused's expectation of privacy is one which society believes is reasonable.

At trial, the military judge held (later overturned) that there was no expectation of privacy because:

> ... (1) the e-mail could not be recalled or erased once it was dispatched and the sender was powerless to keep it from being forwarded; (2) the e-mail messages were transferred to screen

---

[54] *Monachan*, supra note 47.

[55] *Lubovac*, supra note 48.

[56] *United States v. Marshall*, 42 M.J. 568 (A.F. Ct. Crim. App. 1995).

> names rather than to known individuals; and (3) the forwarding of messages to multiple individuals made the situation analogous to bulk mail.

He concluded that the accused was seeking anonymity rather than privacy when he sent the e-mail messages to other users.

The Military Court of Appeal overturned the judge's finding and held that, while the accused may have forfeited his right to privacy to any e-mail transmissions that were downloaded from the computer by another subscriber or removed by an individual from the online service, he nevertheless maintained an expectation of privacy in any e-mail transmissions while they were stored on the online service's computers. The court held that the accused:

> ... clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that [the accused's] computer transmissions would be received by anyone other than the intended recipients.[57]

While it is unclear how the issue would be decided in a Canadian court, both the trial and appeal judgments provide a clue as to the types of factors that a court may consider in determining whether e-mail is a private communication.

(ii) Access Provider:

The access provider could be liable for obscenity distribution for its role in facilitating the e-mail communication. See the discussion above of access provider liability for distribution. It would be difficult to envisage a situation, however, where the access provider would be liable if the subscriber escapes liability on the basis of "private communication".

---

[57] The court referred to *United States* v. *Parrillo*, 34 M.J. 112 (C.M.A. 1992); *United States v. Sturdivant*, 13 M.J. 323 (A.F. Ct. Crim. App. 1995); and *United States* v. *Sullivan*, 38 M.J. 746 (A.C.M.R. 1993).

(iii) Recipient:

The recipient will only be liable for the obscene materials if it forwards the material to another subscriber, in which case it will find itself with the same liability as the original sender of the e-mail, discussed above. Leaving the obscene message in the e-mail "in box", downloading it to disk, or printing a hard copy will probably not lead to criminal liability under section 163. If the obscenity is one that depicts children, the recipient may be liable for possession of child pornography under subsections 163.1(4), as discussed in the child pornography study.

Relevant Legislation

Subsections 163(1) and 163(2) of the *Criminal Code*

Relevant Case Law

R. v. Monachan (1981), 60 C.C.C. (2d) 286 (Ont. C.A.), affd 16 C.C.C. (3d) 576)
R. v. Lubovac (1989), 52 C.C.C. (3d) 551 (Alta. C.A.).
United States v. Marshall, 42 M.J. 568 (A. F. Ct. Crim. App.1995)

Self-aide Practices

(i) Subscriber:

The subscriber could minimize its risk by:

(1) educating itself on the difference between pornography and obscenity;[58]

(2) screening the contents of any materials that it is intending to transmit to ensure that it does not contain obscenity; and

(3) encoding potentially offensive content.

(ii) Online Service Provider / Access Provider:

The online service provider or access provider could minimize its risk by:

(i) educating itself on the difference between pornography and

[58] Note, however, that a mistake as to whether the material is obscene cannot be a defense: *Regina News Ltd.*, supra note 29; *Metro News*, supra note 4.

obscenity;[59]

(ii) adopting an "Acceptable Use Policy" that expressly forbids the exchange of obscenity or other illegal materials through e-mail or other means ;

(iii) responding to illegal materials brought to its attention, by contacting the user, warning the user about the consequences of sending obscenity; and

(iv) providing encoding and other security means for its subscribers.

Such steps may help the parties establish a due diligence defense to a charge of distribution under subsection 163(1) and to establish a defense based on the claim of "private communication".

6. Content Deemed Legal in Traditional Medium Held Obscene In Electronic Version

Issue

Uncertainty over what constitutes the "context" of an electronic publication may result in a publication that, while legal in its printed format, is declared obscene in its corresponding electronic format. Under the Supreme Court of Canada's obscenity test, to determine whether a particular work is obscene the item must be viewed within the broader context of the "work as a whole".[60] As a result, many publications which contain sexually explicit photographs and drawings have survived the obscenity test on the strength of their articles, with the allegedly obscene materials seen as being merely incidental to the broader literary purposes of the publication as a whole. Pictorial or graphic representations may be somewhat harder to "save" in a magazine, if they are not an integral part of a broader work in the context of its theme. When applied to materials provided over an electronic medium, the context analysis becomes even less clear. The problem stems in part from the unique nature of hyper-text, which makes the questionable text or image easily and quickly severable from the remainder of the electronic publication. Considered in isolation, such explicit sexual text or graphics could result in the central and dominant characteristic being deemed to be the undue exploitation of sex, making it obscene despite its legality in a traditional magazine.

---

[59] See note 58.

[60] *Butler*, supra note 2.

Parties Potentially Liable

The publisher of an electronic publication should realize that as a result of any hyper-text features, the material in an electronic version may pose a greater risk of being held obscene than if found in a corresponding print magazine. The publisher may be liable for publication or distribution under subsection 163(1), or selling or exposing to public view under subsection 163(2) for materials that, based on the publisher's past experience in the magazine or print industry, would not have raised any cause for alarm.

Relevant Legislation

Subsections 163(1) and (2) of the *Criminal Code*

Relevant Case Law

R. v. Butler (1992) 70 C.C.C. (3d) 129, 11 C.R. (4th) 137 (S.C.C.)

Self-aide Practices

The publisher should analyze each Web page as a separate publication and assess the legality of the potentially obscene items in the context of only the rest of the page, if the page can be accessed directly by hyper-text link, bypassing the "work as a whole".

7. Posting Or Facilitating Access To Content Which is Illegal In Other Jurisdictions

Issue

A Canadian user, information provider, or access provider posting or facilitating access to content which, while legal in Canada, may be illegal in other jurisdictions which can access the content.

Parties Potentially Liable

The party supplying or posting the information may be liable for violating a foreign jurisdiction's differing obscenity laws, whether that party is a subscriber, BBS operator or newsgroup moderator. The access provider may similarly be liable for its role in facilitating the transmission containing obscene materials. In each case, the accused may be held accountable to not only the widely varying laws, but also the unique community standards of the foreign jurisdiction. Several U.S. cases have held that a party subjects itself to the laws of another state or jurisdiction by

permitting users in that jurisdiction or state to access its service.[61] In *Sable*, the court held that because the operator of a dial-a-porn service was free to tailor its messages on a selective basis, to the communities it chooses to serve, then it must meet those local jurisdictions laws. *Thomas* applied this principle to a BBS operator having subscribers in various states, holding that if the operator wants to provide services to a particular jurisdiction, it is under an obligation to screen its materials to ensure that the materials accessible to that jurisdiction conform with its community standards. The defendants' ability to control access and subscriptions to their BBS made them liable for the downloading of material that occurred in another state and thus subject to the jurisdiction of the courts in such state. Although these cases dealt with inter-state rather than inter-country transmissions, similar principles may also be applied to transmissions crossing national borders.

Relevant Legislation

Each foreign jurisdiction's particular obscenity laws

Relevant Case Law

United States v. Thomas, 74 F. 3d 701 (6th Cir. 1995)
Sable Communications of Calif., Inc. v. F.C.C., 492 U.S. 115, (1989)

Self-aide Practices

The information provider or access provider could minimize its risk by:

(i) educating itself on the difference between pornography and obscenity in all the various jurisdictions to which it provides access or content (a tall order);

(ii) limit access to individual content, newsgroups or mailing lists which may infringe other jurisdictions' criminal laws on either a jurisdiction by jurisdiction basis or by adopting the standards of the most restrictive jurisdiction;

(iii) adopting a procedure for screening online content;

(iv) adopting an "Acceptable Use Policy" that expressly forbids the exchange of obscenity or other illegal materials and requires its users to immediately notify the information provider of any illegal materials found on the system;

---

[61] *United States v. Thomas*, 74 F. 3d 701 (6th Cir.1995); *Sable Communications of Calif., Inc. v. F.C.C.*, 492 U.S. 115, (1989).

(v) upon becoming aware that particular materials are potentially obscene, immediately assess the content and, if possible, delete any illegal materials from its system and post a notice to all subscribers regarding the incident and the action taken;

(vi) warning citizens of other jurisdictions that the content is not screened for such jurisdictions and may contravene local laws;

(vii) encoding potentially offensive content so that users seeking to view the contents are forced to take affirmative steps (such as decoding) in order to view the material;

(viii) requiring a password to access the “adult” portions of the BBS, or newsgroup; and

(ix) blocking access altogether to certain jurisdictions.

[Cat. No.: C2-312/1997E ISBN: 0-662-25489-9]

CHILD PORNOGRAPHY

I. PROHIBITED CONDUCT

1. Overview of Applicable Law on Child Pornography

GENERAL:

The Canadian Criminal Code, the only legislation to deal with child pornography, exhaustively defines in Section 163.1 the various offences relating to this area. Child pornography is defined as any visual representation depicting a minor (i.e. under the age of 18 years) engaging in sexual activity, or having as its dominant characteristic the depiction of a minor's sexual organs or anal region, or any written material or visual representation advocating or counseling such illegal sexual activity with a minor.[1]

Section 163.1 is broken down into three key activities: publication, distribution and possession of child pornography. Subsection 163.1(2) makes it an offence to make, print, publish, or possess for the purpose of publication child pornography. Subsection 163.1(3) targets distribution and prohibits importing, selling or possessing child pornography for the purpose of distribution or sale. Mere possession, regardless of whether it is for the purpose of publication or distribution, is an offence under subsection 163.1(4).

A person charged under s. 163.1 may raise defenses of public good,[2] reasonable mistake of fact,[3] artistic merit, or educational, scientific or medical purposes.[4] The following discussion will assume that these defenses do not apply in each case, unless specifically noted otherwise.

---

[1] *Criminal Code*, s. 163.1(1)

[2] *Criminal Code*, s.163.1(7).

[3] Mistake of fact is only a defence if the accused too all reasonable steps to ascertain the person's age and to ensure that the representation did not depict that person as being a minor: *Criminal Code*, s.163.1(5).

[4] *Criminal Code*, s.163.1(6).

Knowledge Requirements :

As s. 163.1 is a relatively new section, its provisions have not yet been extensively commented upon. The primary uncertainty lies in the type of "mens rea" or mental element that may be required by each of the three offences. There appear to be several approaches that courts may take in interpreting s. 163.1.

As an aid, the courts may look to the interpretation of the corresponding "obscenity" provisions in s. 163. *In Re Paintings etc*, the Ontario District Court held that as s. 163.1 appears to closely parallel s. 163, the child pornography provisions should be interpreted in accordance with the corresponding provision s. 163. Similarly, a B.C. Provincial Court recently held that, as distribution of obscenity has been held to be a strict liability offence then the publication of child pornography must also be a strict liability offence, without going into any further analysis. These assumptions may be problematic because of the different ways in which the two sections are drafted.[5]

In particular, s. 163 groups publication and distribution of obscene materials together under subsection 163(1), clearly distinct from selling obscene materials under subsection 163(2). This distinction is significant, as subsection 163(1) has been held to be a strict liability offence (the only mental element being intent to cause the act), while subsection 163(2) requires in addition a subjective knowledge of the nature and content of the obscene materials. As a result, an important issue in many obscenity cases has been the distinction between distribution and sale, discussed in greater detail in the Obscenity section of this study. Although for child pornography, s. 163.1(3) groups distribution with selling, while publication is included under a separate provision (s. 163.1(2)), the term "knowingly" is not used for either offence.

If the B.C. Provincial Court's decision is based solely on the fact that publication is associated with distribution under what has been held to be a strict liability offence in s. 163, would this automatically mean that associating distribution with selling in s. 163.1(3) makes selling, in the context of child pornography, a strict liability offence? The answer is unclear.

Alternatively, it is possible that a court may interpret s. 163.1(3) by looking at each component individually. In other words, "distribution" may be deemed to be a strict liability offence, while "selling" in the same provision may require a subjective knowledge. This interpretation would make the two offences consistent

---

[5] *In Re Paintings, drawings and photographic slides of paintings* [1995] O.J. No. 1045 [court file No. U219/94]; *R. v. Hurtubise*, Unreported, June 28, 1996, B.C. Prov. Ct., Surrey Registry

with the way they have been interpreted in s. 163. Interpreting s. 163.1 with reference to s. 163 leads to these conflicting possibilities.

> Another approach may be to look to the Obscenity section for the meaning of the particular terms, but to interpret the mens rea requirements in accordance with the more traditional reasoning used by the Supreme Court of Canada in the *Sault Ste. Marie* case[6]. The Court held that where an offense fails to specify the mens rea requirement for the particular offence, there is a presumption that the offence requires a full (or subjective) mens rea unless otherwise provided. Full mens rea requires that the act be committed intentionally[7] or through recklessness[8] or wilful blindness.[9] Mere negligence, while sufficient for a strict liability offence, would not be enough for a full mens rea offence.[10] On this basis, each of the offences in s. 163.1 would appear to require a subjective knowledge and would not be strict liability offences, unlike distribution and publication under s. 163.
>
> As a result of this uncertainty of interpretation, the discussion below will leave open the possibility that publication, distribution and sale of child pornography may each be held ultimately to be either a strict liability or a subjective mens rea offence, and will note the consequences resulting from either option.
>
> Any review of this area of child pornography should be undertaken jointly with a reading of the prior section on obscenity, which canvases some of the following issues in greater detail.

---

[6] *R. v. City of Sault Ste. Marie* (1978) 40 C.C.C. (2d) 353 (S.C.C.).

[7] An accused does an act "intentionally" when he does so for the purpose or desire of bringing about the prescribed harm. In this situation, intent exists regardless of whether the act will certainly, probably or only possible cause the harm. Additionally, this includes an accused who does an act with the intent, purpose or desire of bringing about something other than the prescribed harm, where the accused also foresees that the prescribed harm is certain or substantially certain to occur; *R. v. Chartrand* (1994), 91 C.C.C. (3d) 396 (SCC).

[8] "Recklessness" is where the accused knows or foresees that the prescribed h arm may possibly or probably occur, but is not certain to occur. The accused has no desire for the harm to occur, or may be indifferent as to whether it occurs or not, but nevertheless goes ahead with the act, thereby taking the risk of causing the harm: *R. v. Buzzanga* (1979) 49 C.C.C.(2d) 369 (Ont.C.A.).

[9] "Wilful blindness" arises where a person who has become aware of the need for some inquiry declines to make the inquiry, because he does not wish to know the truth: *Sansregret* v. R. (1985) 18 C.C.C. (3d) 223 (S.C.C.). The test for wilful blindness is a subjective test, focusing on whether the accused was suspicious but deliberately failed to make further inquiries, rather than whether the accused should have been suspicious: *R. v. Currie* (1975), 24 C.C.C. (2d) 292 (Ont. C.A.).

[10] *Sault Ste. Marie*, supra note 6.

2. Application to Internet Activities

The definition of "child pornography" refers to "a photographic, film, video *or other visual representation*, whether or not it was made by electronic or mechanical means"[11] and "any written material or visual representation that advocates or counsels sexual activity" with a person under 18 years of age. The definition is significant for two reasons. First, while it will apply to graphic, video or text files on the Internet, it does not appear to extend to sound files. Second, the reference to making by "electronic or mechanical means" would seem to be broad enough to include computer-simulated child pornography.[12]

To date, there have only been two decided Canadian cases that have considered the obscenity provision in the context of online communications.[13] A third case is pending before the British Columbia Provincial Court, with the decision due to be released in the fall of 1996.[14] In *Pecciarich*, a BBS co-system operator was charged under both the *Criminal Code* obscenity and child pornography provisions for uploading files to the bulletin board. *Hurtubise* and *Clark* are similar cases in which the operators of adult BBSs were charged with both obscenity and child pornography in the content supplied to their subscribers. As all three cases deal only with computer bulletin boards, their application to other Internet activities remains uncertain. However, they offer a valuable starting point for analysis, as discussed in the following sections.

Distribution

Both *Hurtubise* and *Pecciarich* suggest that a BBS can be a distributor, whether for the purposes of subsections 163(1) or 163.1. The decision in *Hurtubise*, however, is being appealed, partially on the basis that the trial judge erred in classifying a BBS as a distributor rather than a retailer.[15] Both decisions, being only at the Provincial Court level, are not binding on higher courts.

---

[11] *Criminal Code*, subsection 163.1(1)(a).

[12] Computer-simulated pornography involves scanning images of children into a computer and manipulating them to depict children in a sexual context, without the use of actual children in any stage of its production.

[13] *R. v. Pecciarich* (1995) 22 O.R. (3d) 748 (Ont. Prov. Ct.) and *R. v. Hurtubise* supra note 5.

[14] *R. v. Clark*, B.C. Prov. Ct.

[15] *Hurtubise* appeal is to be heard in December, 1996.

Although a video store analogy seems appropriate for the various participants in the Internet context, it was rejected by the court in *Hurtubise,* as being inapplicable to a computer bulletin board. The court applied a broad dictionary definition of "distribution" that included "to deal out, give share of each of a number, spread about, scatter, put at different points, divide into parts, arrange, classify", and concluded that the BBS clearly fell within this definition. The judge appears to have been influenced by several factors, in particular the number of people who could access the service, the potential for the information to exponentially spread to further parties, and the ability to make tangible copies of the illegal material:

> "By making a CD accessible through a local computer bulletin board, the contents of the CD become readily accessible to multiple computers. Around each computer, there would be multiple users. The contents of each file on the CD can of course, be downloaded, kept on the computer, copied to another disk, uploaded to other systems, or put into hard print. This is not, in my view, analogous to an individual retailer who is selling individual copies, even if multiple copies, of books or movie video cassettes."[16]

As these factors appear to be equally applicable to newsgroups, Web sites and possibly mailing lists, a court could use similar reasoning to hold that supplying information through these applications also constitutes "distribution".

Another comment on "distribution" in the context of a BBS, is the court's holding in *Pecciarich* that "... evidence of the uploading of the files onto bulletin boards, which the public can access through an application process, is clear evidence of distribution."[17] The reference to "application process" qualifies this ruling more than that in *Hurtubise* and leaves its applicability to newsgroups or Web sites that have no similar application process unclear. However, other than this reference in the above quotation, the application process did not appear to be a significant factor in the decision and could be interpreted by subsequent courts as being immaterial.

Ultimately, the question of whether an act qualifies as "distribution" or retail "sale" may not be an issue in terms of child pornography, since both terms are found in the same subsection 163.1(3) and could , as discussed above, be interpreted

---

[16] *Hurtubise*, supra note 13.

[17] *Pecciarich*, supra note 13.

similarly for purposes of the required mens rea. The importance of the difference is far clearer and greater for obscenity offences under section 163.

Publication

On the issue of publication, the court in *Hurtubise* once again once relied on a broad dictionary definition, that included "making publicly known; issuing of book, engraving, music, etc., to the public." The court concluded that the defendants possessed the obscene material for the purpose of publication "... because of the capabilities of the computer to show material to a number of parties and to produce material easily and inexpensively ..."[18] The reference to "computer", and the ability of other Internet applications to provide easy, inexpensive access to large numbers of people, suggest that information supplied by newsgroups, mailing lists and Web sites may similarly be held to be "publication".

Possession

Possession is defined generally in s. 4 for the purpose of various offences in the *Criminal Code*. A person is in possession of an item when (a) it is in that person's personal possession; or (b) the person knowingly has it in the actual possession of another person; or (b) the person knowingly has the item in a place for the use or benefit of himself or another person.[19]

The courts have interpreted possession as requiring both knowledge and control.[20] Both elements must be present at the same time. For example, mere manual handling of an object, even if coupled with control, is insufficient to prove possession if the accused is unaware that he is handling something which is illegal to possess.[21] There is also no possession where the accused has both knowledge and a right of control over an object but does not *intend* to exercise the control.[22] This would be the case, for example, when an accused was merely "manually

---

[18] *Hurtubise*, supra note 13.

[19] *Criminal Code*, s. 4[3](3).

[20] *Beaver v. R.*, [1957] S.C.R. 531; *R. v. Lawrence* (1952), 13 C.R. 425 (Ont. C.A.); *R. v. Hess (No. 1)* (1949), 8 C.R. 42 (B.C.C.A.);

[21] Ibid.

[22] *R. v. Christie* (1978), 41 C.C.C. (2d) 282 (N.B.C.A.).

handling" the materials in order to pass them on to another party.[23]

Applying these cases to Internet communications, it may be possible to argue that third parties who merely facilitate or transmit messages for their subscribers [24] are simply passing (in a technical sense) the messages on to other parties, with no intention of exercising "editorial" control over them. On this basis, such third parties could be held not to be in "possession" of the messages for the purposes of the *Criminal Code*. Perhaps even more importantly, a party such as an access provider who had no knowledge of the true character of a message containing child pornography would not be liable for possession under s. 163.1(4), unless it was deemed to have exercised wilful blindness.[25]

Due Diligence

If any of the three categories of offences under s. 163.1 are deemed to be strict liability offences, the Crown will not be required to prove that the accused had knowledge of the existence and nature of the child pornography. However, it will still be open to the accused in such a case to avoid liability by showing that he or she exercised due diligence, or reasonable care, in the circumstances.[26] Though the court in *Hurtubise* found that the accused did not exercise due diligence, its comments on what the defendants failed to do indicate the kinds of factors a court might consider when assessing due a diligence defence:

---

[23] Ibid.

[24] This may include, for example, Internet access providers, online services, submission moderators, and BBS, newsgroup or mailing list operators.

[25] See note 9, above.

[26] *R. v. Metro News Ltd*. (1986) 20 C.C.C. (3d) 35 (Ont. C.A.).

> "Although they made efforts to ascertain how they could restrict access to adult users, they made no effective inquiries as to content. They did not obtain any advice as to the meaning of "obscenity" and did not distinguish between pornography and obscenity. They did, however, clearly recognize that some of the material which people were transmitting was offensive ... Even after being alerted to this kind of material they made no effort whatsoever to review the material on [their own] CD. They did not review the file names in the directories, any sampling of the material on the CD, nor even look at what was contained on the CD."[27]

[27] *Hurtubise*, supra note 13.

II. ACTIVITIES AT RISK

1. Access Provider's Facilities Used to Transmit Child Pornography by its Users

Issue:

An access provider that merely provides users with a connection to the Internet may nevertheless be liable for child pornography transmitted by its users.

Party Potentially Liable:

The provider may be liable, if not for publication under subsection 163.1(2), then arguably at least for distribution under subsection 163.1(3) for its role in transmitting the child pornography. If distribution is deemed to be a strict liability offence, the provider may be liable even if it was not aware of the nature of the illegal materials, though it could avoid liability by showing that it exercised due diligence in the circumstances.[28] On the other hand, if distribution of child pornography is deemed to be an offence requiring a subjective mens rea, the Crown will have a fairly high threshold of showing that the provider distributed the child pornography intentionally,[29] recklessly[30] or through wilful blindness.[31]

If the provider's server or other hardware, for whatever reason, retains a copy of the materials transmitted by its users, the provider could also be liable for possession of child pornography under subsection 163.1(4). The provider may be able to avoid liability for possession by proving that (1) it lacked knowledge of the presence and character of the child pornography;[32] (2) it lacked control over its users' communications;[33] or (3) although it had a right of control over the communications equipment, it had no intention of exercising control over the

---

[28] See discussion of due diligence above.

[29] See note 7, above.

[30] See note 8, above.

[31] See note 9, above.

[32] See text accompanying notes 20 and 21, above.

[33] See text accompanying note 20, above.

content.[34] These defenses depend on the fact that an access provider does not pre-screen material before transmitting it to its intended location, and as such is not in a position to prevent the transmission of child pornography through its server. The access provider would need to be careful, however, that its lack of knowledge or control is not deemed to constitute wilful blindness, particularly after it is advised of the existence of any child pornography content.

Relevant Legislation:

Criminal Code, s. 4(3), s. 163.1(3), s. 163.1(4)

Relevant Case Law:

R.. v. Hurtubise, Unreported, June 28, 1996, Surrey Registry, B. C. Prov. Ct.

Self-Aide Practices:

The access provider could minimize its risks by:

(i) obtaining a legal opinion as to what constitutes child pornography;

(ii) adopting an "Acceptable Use Policy" that forbids users to transmit illegal material;

(iii) establishing a policy for dealing with users found to be transmitting such illegal materials.[35]

Taking these steps may help the provider establish a due diligence defense, or a defense to charges of recklessness or wilful blindness.

---

[34] See text accompanying notes 22 and 23, above.

[35] For example, the policy could range from issuing a warning, to suspending the users' privileges, to terminating their accounts.

2. Child Pornography Supplied by Information Provider

Issue:

An information provider may itself post content containing child pornography to its bulletin board, web site, newsgroup or online service. The information provider may or may not know that the content contains pornography that is illegal. Operators of adult BBSs in particular, may supply what, on the whole, appears to be legal pornography, without realizing that it contains depictions of persons under 18 years. This can be due to either a lack of understanding of what constitutes child pornography or a failure to adequately screen the materials.

Parties Potentially Liable:

(i) Information Provider:

Evidence that the information provider uploaded the materials will likely be evidence of distribution.[36] On the basis of *Hurtubise*, the information provider may be liable for publication under subsection 163.1(2), or for distribution (or selling) under subsection 163.1(3).[37] If distribution and publication are deemed to be strict liability offences, the information provider may be liable, even if it had no knowledge of the child pornography, although it may be possible to avoid liability by showing that it acted with due diligence in choosing its materials content.[38] On the other hand, if publication and distribution require a subjective mens rea, the Crown will need to prove that the information provider knew of the child pornography, or was reckless[39] or wilfully blind[40] to the possibility of child pornography being included in the content that it was supplying.

If the child pornography remains on the information provider's server, the information provider may also be held liable for possession under s. 163(4). In such a case the provider may be able to avoid liability for possession by

---

[36] *Pecciarich,*, supra note 13.

[37] *Hurtubise*, supra note 13.

[38] See discussion of due diligence above.

[39] See note 8, above.

[40] See note 9, above.

suggesting that (1) it lacked knowledge of the presence and character of the child pornography;[41] (2) it lacked control over its users' communications;[42] or (3) although it had a right of control over the communications, it had no intention of exercising control over the content.[43] An information provider would also need to be careful, when making this argument, that its lack of knowledge or control was not wilful blindness.

(ii) Access Provider:

If the information provider uses a separate access provider for its connection to the Internet, the access provider may itself be liable for child pornography as discussed above.

Relevant Legislation Case:

Subsections 163.1(2), (3) and (4) of the *Criminal Code.*

Relevant Case Law:

R. v. Pecciarich (1995) 22 O.R. (3d) 748 (Ont. Prov. Ct.)

R. v. Hurtubise, Unreported, June 28, 1996, Surrey Registry, B. C. Prov. Ct.

Self-aide Practices:

Self-aide practices will obviously not help the provider who willingly supplies child pornography with the knowledge that it is clearly illegal .

On the other hand, the information provider who unwittingly posts child pornography with the intent of posting only legal materials could minimize its risk of lability by:

(i) educating itself on what constitutes child pornography;

(ii) adopting a procedure for screening online content (for example, screening individual files before posting);

---

[41] See text accompanying notes 20 and 21, above.

[42] See text accompanying note 20, above.

[43] See notes accompanying notes 22 and 23, above.

(iii) adopting an "Acceptable Use Policy" that expressly forbids the exchange of child pornography or other illegal materials and requires its users to immediately notify the information provider of any illegal materials found on the system;

(iv) adopting a procedure for responding to illegal materials - for example, upon becoming aware that particular materials may constitute child pornography, the provider should immediately assess the content and delete any suspect materials from its system, notify the user who posted the material and post a notice to all subscribers regarding the incident and the action taken;

(v) posting warnings of potentially offensive content being accessible on the system.

(vi) encoding potentially offensive content, so that users seeking to view the contents are forced to take affirmative steps (such as decoding) in order to view the material; and

(vii) requiring a password to access the "adult" portions of the BBS, newsgroup, Web site or online service.

There is some prospect that such actions may help the information provider to establish a due defence or rebut allegations of recklessness or wilful blindness under subsections 163.1 (2) or 163.1(3).

3. Child Pornography Posted to Newsgroup or BBS by Subscriber

Issue:

A subscriber posts content containing child pornography to a newsgroup or bulletin board.

Parties Potentially Liable:

(i) Subscriber:

While the only authority dealing with "distribution" and "publication" in an online context considered a BBS rather than a newsgroup, there do not appear to be any significant distinguishing features that would make posting to a newsgroup less of a "publication" or "distribution" than one to a BBS. The subscriber who posted the material may be liable for publication under subsection 163.1(2) or distribution under subsection 163.1(3). There is less prospect of that occurring of course, if the subscriber is located outside of Canada or cannot be readily identified.[44] It is not clear whether publication and distribution are strict liability offences, or whether they also require an element of subjective mens rea. However, since the act of posting or being the source of the material suggests to some degree that the subscriber was aware of the nature and content of the material, it may be more difficult for the subscriber to establish due diligence[45] or lack of knowledge as a defense. If the subscriber retained a copy of the obscenity on its hard drive, printed it or saved it to disk, the subscriber may also be liable for possession under subsection 163.1(4). It would likely be difficult in this case to establish that the subscriber lacked the knowledge or control to constitute possession required under the *Criminal Code*.[46]

---

[44] For example, subscribers may not be readily identifiable if they posted the material through an anonymous remailler.

[45] See discussion of due diligence above.

[46] See text accompanying note 20 to 23, above.

(ii) Newsgroup or BBS Operator:

The liability of an operator for the content posted to its newsgroup or bulletin board may depend on whether the operator is located in Canada and whether the newsgroup or BBS is moderated or unmoderated. For both moderated and unmoderated newsgroups or bulletin boards, the operator may potentially be liable for either publication or distribution of child pornography. If the offences are deemed to be strict liability offences, the operator may be liable even if it didn't know of the existence or nature of the child pornography, although it could avoid liability by showing that it exercised due diligence.[47] On the other hand, if publication and distribution are deemed to require subjective mens rea, the Crown will need to prove that the operator knew of the child pornography, was reckless[48] or was wilfully blind to it.[49]

(1) Moderated Newsgroup or BBS:

In spite of the fact that there have not yet been any cases on this point, it seems possible that a court would hold that a newsgroup or BBS operator who uses a submission moderator to review subscribers' postings should have been in a position to have known whether the postings contained child pornography. The operator's failure to remove the illegal materials would likely be seen as recklessness,[50] wilful blindness [51] or a lack of due diligence,[52] thus making it liable for publication and/or distribution, regardless of whether they were treated as strict liability or subjective mens rea offences.

Because the due diligence standard does not demand perfection, a court may recognize that despite an operator's reasonable efforts to prevent illegal postings, child pornography may occasionally

---

[47] See discussion of due diligence above.

[48] See note 8, above.

[49] See note 9, above.

[50] See note 8, above.

[51] See note 9, above.

[52] See discussion of due diligence.

"slip through the system", and hold that the operator should not be liable.

If the child pornography is saved on the operator's computer, the operator may be liable for possession under s. 163(4). This is because a moderated newsgroup contemplates that the operator exercise control over the users' messages. The operator will not be able to raise a lack of intent to control the messages as a defense in this circumstance.[53] It may still be possible to avoid the charge by showing that the operator had no actual knowledge of the existence of child pornography,[54] although the operator must be careful that this lack of knowledge is not characterized as wilful blindness.

***(2) Unmoderated Newsgroup* or BBS:**

It is likely that the operator of an unmoderated newsgroup or bulletin board will be liable for publication, distribution and possession under section 163.1, if it had knowledge or reason to believe that child pornography was being posted. However, it will have a greater chance of avoiding liability through any of the defenses based on lack of knowledge, control or intent to control than would an operator of a moderated newsgroup or BBS.[55]

(iii) Submission Moderator:

No cases have dealt with this issue. It seems reasonable to assume however, that a submission moderator could be liable for publication or distribution under 163.1, on the basis that the moderator's role of accessing and reviewing postings provides the moderator with both the specific content knowledge and the ability to delete or to permit the content to be posted. The Crown would have to prove that the submission moderator's actions actually constituted "publication" or "distribution" as opposed to simply contributing to them. While these terms may likely encompass the activities of the operator of a BBS or newsgroup, they will be more difficult to apply to the activities of a submission moderator. Depending on whether publication and distribution are deemed strict liability or

---

[53] See text accompanying note 22 and 23, above.

[54] See text accompanying notes 20 and 21, above.

[55] See text accompanying notes 20 to 23, above.

subjective mens rea offences, the moderator could respond to these charges by showing that it acted with diligence,[56] or was neither reckless [57] nor wilfully blind, particularly if it alerted the operator.[58]

(iv) Access Providers:

The reference here is to Internet newsgroups in general ("Usenet") rather than newsgroups confined to the subscribers of a particular BBS or online service. The mode of Usenet newsgroups operations makes it impossible for any one site to effectively exercise editorial control over the postings by the newsgroup's subscribers.[59] The access provider's control is thus limited to either offering or blocking access to a particular newsgroup.

With no cases dealing with this point, it is uncertain whether an access provider's decision to provide access to a newsgroup handling child pornography could be deemed to be an affirmative act sufficient to constitute distribution under 163.1(3). If distribution is deemed to be a strict liability offence, the provider may be liable even if it was not aware of the child pornography. If, on the other hand, it requires a subjective mens rea, the Crown will need to prove that the access provider distributed the child pornography intentionally, recklessly[60] or through wilful blindness.[61] It is arguable that the access provider's failure to block a newsgroup carrying child pornography may be seen as a lack of due diligence, recklessness or wilful blindness, particularly if the newsgroup's history or character provides the access provider with a reason to believe that the newsgroup will deal with illegal materials, such as those in the *alt.sex.binaries* hierarchy. As well, if the access provider becomes aware of child pornography being posted to a newsgroup but fails to block access to the newsgroup subsequent to the discovery, there is a greatly enhanced prospect of liability. If a copy of the child pornography is saved on the access provider's server, it may also become liable for possession under subsection 163.1(4).

---

[56] See discussion of due diligence above.

[57] See note 8, above.

[58] See note 9, above.

[59] The operator administering the Usenet newsgroup may not necessarily be in Canada, and may or may not be known to the access provider.

[60] See note 8, above.

[61] See note 9, above.

The provider may seek to avoid liability by suggesting that it lacked knowledge of the presence and character of the child pornography;[62] that it lacked control over its users' communications;[63] or that even though it had a right of control over the communications, it had no intention of exercising the control.[64] All of these defences will depend on the particular facts of each case to sustain them.

(v) Universities as Access Providers:

Although universities are only one type of access provider, they possess certain unique characteristics that make it useful to examine their liability within a separate context. In that respect, see the discussion dealing with Universities under the Obscenity report, which suggests that due to the *Canadian Charter of Rights and Freedoms*, a university may not be under an obligation to ban a newsgroup solely on account of offensive content - leading to the conclusion that a university's decision to continue offering access to the newsgroup would not be seen as a lack of due diligence or as being reckless or wilfully blind.

Relevant Legislation:

Criminal Code, s. 4(3), s. 163.1(2), s. 163.1(3) and s. 163.1(4)

Section 2(b) of the *Canadian Charter of Rights and Freedoms*

Relevant Case Law:

U.S. v. Thomas, 74 F.3d 701, 1996 U.S. App. LEXIS 1069 (6th Cir. 1996)

United States v. Lacy, CR95-297WD (W.D. Wash. 1995)

---

[62] See text accompanying notes 20 and 21, above.

[63] See text accompanying note 20, above.

[64] See text accompanying notes 22 and 23 above.

Self-aide Practices:

(i) Subscriber

The subscriber or submission moderator could minimize its risk by:

(1) educating itself on what legally constitutes child pornography; and

(2) screening the contents of any materials to be posted prior to forwarding them.

(ii) Newsgroup Operator / BBS Operator / Submissions Moderator / Access Provider

The newsgroup operator, BBS operator moderator and access provider could minimize its risk of liability by:[65]

(i) educating itself on what legally constitutes child pornography;

(ii) adopting a procedure for screening online content:

(iii) adopting an "Acceptable Use Policy" that expressly forbids the exchange of child pornography and requires immediate notice of any illegal materials found on the system;

(iv) adopting a procedure for responding to illegal materials by assessing the content, if possible deleting any illegal materials from its system, and posting a notice to all subscribers regarding the incident and the action taken;

(v) posting warnings of potentially offensive content;

(vi) encoding potentially offensive content so that users seeking to view the contents are forced to take affirmative steps (such as decoding) in order to view the material; and

(vii) requiring a password to access the "adult" portions of the BBS, or newsgroup.

---

[65] Some of the suggestions, such as the ones in (ii) and (iv), may be more appropriate for the newsgroup or BBS operator than for the access provider.

One or more of such steps may help the parties establish a due diligence defense, or assist in proving a lack of recklessness or wilful blindness for purposes of subsections 163.1(2) or 163(3).

4. Child Pornography Transmitted Through Mailing List

Issue:

A subscriber in Canada transmits content containing child pornography directly to other mailing list subscribers.

Parties Potentially Liable:

(i) Subscriber:

The subscriber's liability for publication, distribution, and possession of child pornography will likely be similar to that of a subscriber who posts child pornography to a newsgroup or BBS, as discussed in section above.

(ii) Mailing List Operator:

The liability of the operator will depend on whether the mailing list operator is located in Canada, and the mailing list is open, moderated, unmoderated or closed.

***(1) Open Mailing List - Moderated*:**

The liability of an operator of a moderated open mailing list will likely be similar to that of a moderated newsgroup operator, as discussed above.

***(2) Open Mailing List - Unmoderated*:**

The liability of an operator of an unmoderated open mailing list will likely be similar to that of an unmoderated newsgroup operator, as discussed above.

***(3) Closed Mailing List*:**

The liability of a closed mailing list operator may depend on

whether the mailing list is considered a "private medium".[66] In response to a charge of publication under subsection 163.1(2) or distribution under subsection 163.1(3), the operator could seek to distinguish the mailing list from other modes of distribution or publication by stressing that a mailing list is a "private communication" which lacks the essential "public" element. See the first three paragraphs of the discussion concerning the same subject under the Obscenity report.

The mailing list operator may also be potentially liable for possession of child pornography under subsection 163.1(4), but could seek to avoid liability by showing that it lacked either knowledge of the child pornography, control over its users' messages, or intent to exercise control over its users' messages.

(iii) Submission Moderator:

The liability of the mailing list's submission moderator will likely be similar to that of a newsgroup's submission moderator, as discussed above.

(iv) Access Provider:

The access provider may be liable for distribution or possession under s. 163.1 for its role in facilitating access to the child pornography material on the mailing list. See the fuller discussion of access provider liability, for the other activities reviewed above.

Relevant Legislation:

Criminal Code, s. 4(3), s. 163.1(2), s. 163.1(3) and s. 163.1(4)

Self-aide Practices:

(i) Subscriber:

The subscriber could minimize its risk by:

(1) educating itself on what constitutes child pornography; and

[66] See below, for a similar discussion in the context of e-mail.

(2) screening the contents of any materials that it was going to be posting to the mailing list, prior to posting.

(ii) Mailing List Operator / Submission Moderator/ Access Provider:

The mailing list operator, moderator and access provider could minimize its risk by:[67]

(i) educating itself on what constitutes child pornography;

(ii) adopting a procedure for screening online content (for example, screening individual files before posting);

(iii) adopting an "Acceptable Use Policy" that forbids the exchange of child pornography or other illegal materials;

(iv) upon becoming aware that particular materials may constitute child pornography, assessing the content, deleting any illegal materials from its system; warning the user who posted the material and posting a notice to all subscribers regarding the incident and the action taken;

(v) posting warnings of potentially offensive content;

(vi) encoding potentially offensive content so that users seeking to view the contents are forced to take affirmative steps (such as decoding) in order to view the material; and

(vii) requiring a password to access the "adult" portions of the BBS, or newsgroup.

Such steps may help the parties establish a due diligence defense or provide evidence of a lack of recklessness or wilful blindness under subsections 163.1(2) or 163.1 (3) is unclear, but appear to offer at least some comfort.

[67] Some of the suggestions, such as the ones in (ii) and (iv), may be more appropriate for the mailing list operator than for the access provider.

5. Child Pornography Transmitted Through E-Mail

Issue:

A subscriber transmits content to one or more persons through e-mail. The issue of liability arises with respect to any child pornography found in either the message itself, or in an attached file.

Parties Potentially Liable:

(i) Subscriber:

The liability of the subscriber sending the e-mail may depend on whether e-mail is considered a private medium.

The subscriber may be liable for publication under subsection 163.1(2) or distribution under subsection 163.1(2), unless the court finds that e-mail is a "private communication". See the fuller discussion on private communications in the Obscenity report.

It is not clear whether publication and distribution are strict liability offences, or whether they require subjective mens rea. However, since the act of sending an e-mail message strongly suggests that the subscriber was aware of the nature and content of the material being sent, it may be difficult for the subscriber to establish due diligence or lack of knowledge defenses, although this will of course depend on the particular facts of each case.

If the subscriber downloads a copy of the child pornography to the hard drive or disk, or prints out a hard copy, the subscriber may also be liable for possession of child pornography under subsection 163.1(4). In such case, it would likely be difficult to establish that the subscriber lacked the knowledge or control to constitute possession under the *Criminal Code*.

(ii) Access Provider:

The access provider may be liable for distribution of child pornography, due to its role in facilitating the e-mail communication. See the discussion of access provider liability for distribution, above.

(iii) Recipient:

A recipient of the e-mail will likely be liable for distribution of child pornography if it deliberately forwards the material to another subscriber, in which case it will find itself in the same role as the original sender of the e-mail, as discussed above. If it retains a copy of the child pornography, the recipient may also be liable for possession under subsection 163.1(4).

Relevant Legislation:

Criminal Code, s. 4(3), s. 163.1(2), s. 163.1(3) and s. 163.1(4)

Self-aide Practices:

(i) Subscriber:

The subscriber could attempt to minimize its risk by:

(1) educating itself on what legally constitutes child pornography; and

(2) screening the contents of any materials that it is intending to transmit by e-mail to ensure that they do not contain child pornography.

(ii) Online Service Provider / Access Provider

The online service provider or access provider could minimize its risk by:

(i) educating itself on what constitutes child pornography;

(ii) adopting an "Acceptable Use Policy" that expressly forbids the exchange of child pornography or other illegal materials through e-mail or other means; and

(iii) adopting a procedure for responding to illegal materials including warning the user about the consequences of sending child pornography in the future

Such steps may help the parties establish a due diligence defense or prove a lack of recklessness or wilful blindness under subsections 163.1(2) or 163.1(3).

[Cat. No.: C2-312/1997E ISBN: 0-662-25489-9]

HATE PROPAGANDA

I. PROHIBITED CONDUCT

1. Overview of Applicable Law on Hate Propaganda

The primary legislation dealing with hate propaganda is the Criminal Code, the Broadcasting Act and various human rights statutes. Due to the limited scope of this study, only the Criminal Code is reviewed in detail.

Criminal Code

The three sections dealing with hate propaganda in the Canadian Criminal Code are sections 318, 319 and 320.

Section 318 ("Advocating Genocide")

Section 318 makes it an offence to *advocate or promote* genocide (killing or inflicting conditions to destroy members of a group). It differs from section 319 in that it is not limited (as is section 20) to statements made in a public place or those made other than in private conversation. Although the meaning of "advocates and promotes" has not yet been tested, we can look for guidance to the Supreme Court of Canada's interpretation of "promotes" in the context of s. 319(2) in *R. v. Keegstra*.[1] "Promotes" was held to mean active support or instigation or something more that mere encouragement or advancement of hatred. It is likely that "advocates and promotes" would be interpreted similarly in s. 318.

Section 319 ("Public Incitement of Hatred")

Section 319 creates two offences.

Subsection (1) targets everyone who *incites hatred* against any identifiable group by *communicating statements in any public place*, where such incitement is likely to lead to a breach of the peace. Section 319 defines "communicating," "statements" and "public place" non-exhaustively. Communicating is defined as including "communicating by telephone, broadcasting or other audible or visible means."[2] Statements include "words spoken or written or recorded electronically

[1] *R. v. Keegstra*, [1990] 3 S.C.R. 697.

[2] *Criminal Code*, s. 319(7).

or electro-magnetically or otherwise, and gestures, signs or other visible representations."[3] Public place includes "any place to which the public have access as of right or by invitation, express or implied."[4] "Incite" has been held to mean to "urge someone to do something" or "stir them up to do something".[5]

Subsection (2) makes it an offence to *willfully promote hatred* against an identifiable group by *communicating statements, other than in private conversation.* The Supreme Court of Canada addressed the meaning of "willfully," "promote" and "other than in private conversation" in *R. v. Keegstra.*[6] The court held that "promotes" involves the active support or instigation of hatred; a simple encouragement or advancement of hatred is not enough.[7] With respect to "willfully, " an accused needs both to *intend*, in the sense of desire, and to *foresee* the stimulation of hatred as a certainty. Neither recklessness[8] nor the mere fact that the accused was aware of the risk of stimulating hatred are sufficient to convict under s. 319(2).[9] A conversation or communication intended to be private but which was accidentally or negligently made public also does not fall under s. 319(2).[10]

Section 320 ("Seizure of Hate Propaganda")

Section 320 permits a court to authorize the seizure of copies of a publication believed to be hate propaganda[11] when the copies are kept for distribution or sale in premises within the court's jurisdiction.[12] If the court is satisfied that the

---

[3] *Criminal Code*, s. 319(7).

[4] *Criminal Code*, s. 319(7).

[5] *R. v. Dionne* [1990], 107 N.B.R. (2d) 38 (N.B.C.A.).

[6] *Keegstra*, supra note 1.

[7] *Keegstra*, supra note 1.

[8] *R. v. Buzzanga and Durocher* (1979), 49 C.C.C. (2d) 369 (Ont. C.A.); applied in *Keegstra*, supra note 1.

[9] *Keegstra*, supra note 1.

[10] *Keegstra*, supra note 1.

[11] There must be *reasonable grounds to believe* that the publication is hate propaganda: *Criminal Code*, s. 320(1).

[12] Ibid.

publication is indeed hate propaganda, it may order that the seized copies be forfeited.[13] "Hate propaganda" is defined for the purposes of s. 320 as " ... any writing, sign or visible representation that advocates or promotes genocide or the communication of which by any person would constitute an offence under section 319".[14]

Human Rights Legislation

Both the federal and provincial human rights acts prevent communications that are likely to expose a person or group of persons to hatred on the basis of a prohibited ground of discrimination. The acts also provide remedial measures to persons who have been exposed to hatred in these circumstances.

(i) ***Canadian Human Rights Act***

Section 13 of the *Canadian Human Rights Act* prohibits the communication of hatred through telephone lines. Subsection (1) states that it is a discriminatory practice to communicate repeatedly "...any matter that is likely to expose a person to hatred or contempt by reason of the fact that that person or those persons are identifiable on the basis of a prohibited ground of discrimination." It applies to "... a person or a group of persons acting in concert to communicate telephonically or to cause to be so communicated repeatedly, ... by means of the facilities of a telecommunications undertaking within the legislative authority of Parliament."[15]

Subsection (1) is inapplicable to any matter that is communicated in whole or in part by means of the facilities of a broadcasting undertaking.[16] Where the telecommunication facilities are used by other persons to transmit hate propaganda, the owners or operators of such telecommunication undertakings are exempted from liability.[17]

---

[13] *Criminal Code*, s. 320(4)

[14] Criminal Code, s. 320(7).

[15] *Canadian Human Rights Act*, s. 13(1).

[16] *Canadian Human Right Act*, s. 13(2).

[17] *Canadian Human Rights Act*, s. 13(3).

(ii) Provincial *Human Rights Acts*

The broadest provincial provision dealing with hate propaganda appears to be s. 14(1) in the *Saskatchewan Human Rights Code*.[18] As s. 14(1) has been upheld as constitutionally valid,[19] it is likely that the courts would similarly uphold the constitutional validity of the other provinces' less stringent anti-discrimination provisions.

(iii) *Broadcasting Act*

A number of regulations under the *Canadian Broadcasting Act* target the promotion of hatred through broadcasting. These sections prohibit a licensee from broadcasting or distributing programming that contains any abusive comment, that when taken in context, tends or is likely to expose an individual, group or class of individuals to hatred or contempt on the basis of a discriminatory ground.[20] The constitutional validity of these provisions has not yet been challenged.

---

[18] Section 14(1) states that no person shall publish or display in a newspaper, through a television or radio broadcasting station or any other device or in any printed matter or publication or by means of any other medium that he owns or controls, any notice, symbol, emblem, article, statement or other representation which exposes, or tends to expose, to hatred, ridicules, belittles or otherwise affronts the dignity of any person because of his or their race, creed, religion, colour, sex, marital status, disability, age, nationality, ancestry or place of origin.

[19] *Saskatchewan Human Rights Commission et al. v. Bell*

[20] *Radio Regulations, 1986*, s. 3(b); *Specialty Services Regulations, 1990*, s. 3(b); *Television Broadcasting Regulations, 1987*, s. 5(b); and *Pay Television Regulations, 1990*, s. 3(b).

2. Application To Internet Activities

As there have not yet been any Canadian or U.S. cases that have applied hate propaganda laws to Internet communications, the only guidance thus far is the wording of the statutes and their interpretation under traditional case law.

Criminal Code, s. 318

Section 318 does not distinguish between the medium of communication used to advocate or promote genocide. Neither is it limited to a public place [21] or communications other than in private communication.[22] The provision contains nothing to preclude it from applying to statements made on bulletin boards, newsgroups, mailing lists, Web sites, e-mail or interactive chat sessions.

However, as "promotes" has been interpreted in other contexts to mean active support or instigation, its applicability appears to be limited to the person actually making the statements, such as a subscriber who posts a message to a newsgroup, BBS or Web site, a user who transmits the message through e-mail, or an information provider who chooses and supplies information directly through its online service. It would likely not include parties who simply enable the statements to be made via their facilities, such access providers, newsgroup or mailing list moderators, or operators of newsgroups, mailing lists or bulletin boards, where the statement promoting and advocating genocide is made by a subscriber or user.

Criminal Code, s. 319(1)

In order for an offence to be committed, the following elements must be present.

(i) "Communicating":

The first half of subsection 319(1) is concerned with "communicating statements in any public place." Communicating is defined as including telephone, broadcasting or other audible or visible means.[23] This definition is broad enough to include Internet text, video, graphic and sound files. It appears not to be limited to the person actually *making* the statement, and probably would extend to a third party,

---

[21] Contrast this with s. 319(1), which only applies to statements made in a public place.

[22] Contrast this with s. 319(2), which only applies to statements communicated other than in private conversation.

[23] *Criminal Code*, s. 319(7).

such as an online service, BBS operator or access provider deliberately supplying the means or facilities for the purpose of making the statement, because the definition of "communicating" is non-exhaustive.

(ii) "Statements":

Statements, defined non-exhaustively as including spoken or written or recorded electronically or electromagnetically, or otherwise, and gestures, signs or other visible representations,[24] appears to be broad enough to include communications made through Internet text, video, graphic and sound files.

(iii) "Public Place":

Although public place is defined as including any place to which the public have access as of right or invitation, express or implied,[25] this definition is far from clear. There appear to be at least four complications in applying the definition of "public place" to Internet communications.

First, does public access mean a place to which *any* members of the public have access or to which *some* members of the public have access?[26] The courts have interpreted public place broadly in other contexts, holding that it is not necessary that all segments of the public have a right of access for it to be a public place.[27] This interpretation seems broad enough to include most Internet communications, with the possible exception of e-mail.

Second, it is not clear from the definition whether public is intended to mean state-owned, as in a public street, or whether it also includes private property. The former definition would exclude most Internet communications, as most online services, bulletin boards and access providers are privately owned. The courts have tended to interpret public place in other contexts as including private property.[28] For example, the New Brunswick Court of Appeal held that where private property was frequented by members of the public with no objection by the owner,

---

[24] *Criminal Code*, s. 319(7).

[25] *Criminal Code*, s. 319(7)

[26] Examples in which some but not all members of the public have access include adult only bulletin boards and general membership online services which require payment of monthly fees.

[27] For example, *Tegstrom v. The Queen* held that a bar from which a portions of the public may be excluded by law or by choice was held to be a public place: *Tegstrom v. The Queen*, [1971] 1 W.W.R. 147 (Sask. D.C.)

[28] A public place is not restricted to a place to which the public has access by right. It includes a place in which the public can witness indecent acts *R .v. Bailey* (1986) 30 C.C.C. (3d) 30.

it was transformed into a public place.[29] It is possible that courts would interpret public place similarly for the purpose of applying s. 319(1) to Internet facilities .

However, even assuming that public place is held to extend to privately owned Internet services, the matter may be further complicated by the fact that in most cases, the subscriber using these services does not actually *go to* that public place; in fact, the user never physically leaves the privacy of his or her home. While users may theoretically be communicating in a *virtual* public place, it is not clear that s. 319(1) was meant to apply to non-physical locations. Cases that have dealt with "public place" in the context of indecent exposure or solicitation for the purpose of prostitution have held that when a person is located on or in his private property, but in view of the public, that person is deemed to be in a public place for the purposes of the offence.[30] Using this analogy, a user communicating through a computer in his private home to a publicly accessible site (e.g. BBS) may be deemed to be "in view of the public" and thus in a public place for the purpose of s. 319(1).

Finally, would the definition of public place extend to a situation where the physical server to which a message is posted is located outside of Canada? This is likely the most difficult question, since while the person communicating the statement may be physically in Canada and the audience to which the statement is communicated may include Canadians, the message may physically reside on a computer beyond the reach of Canadian criminal law. A court may conceivably attempt to get around this extra-territoriality question by interpreting public place broadly to include virtual locations with messages, particularly if they can be downloaded into Canadian computers. In support of this interpretation is a further argument, based on the analogy made in the prior paragraph.

In the absence of clear authority on the application of public place to differing types of Internet communications, the discussion of liability that follows will assume the broadest possible interpretation - public place will be assumed with this study to include all Internet communications by Canadians (other than private e-mail), including those messages posted only to a foreign server provided that they may also be accessible to a Canadian audience.

---

[29] *R. v. Lavoie*, [1968] 1 C.C.C. 265 (N.B.C.A.), in which the court was considering public place in context of s. 150 of the Criminal Code. The definition of public place in s. 150 is identical to the definition in s. 319.

[30] See generally: *R. v. McEwen*, [1980] 4 W.W.R. 85 (Sask. Prov. Ct.); *R. v. Figluizzi* (1981), 59 C.C.C. (2d) 144 (Alta. Q.B.); *R. v. Wise* (1982), 67 C.C.C. (2d) 231 (B.C. Co. Ct.); and *R. v. Smith* (1989), 49 C.C.C. (3d) 127 (B.C.C.A.).

(iv) "Incites hatred ... likely to lead to a breach of the peace":

The second half of s. 319(1) requires that the statement communicated "incites hatred ... where such incitement is likely to lead to a breach of the peace." Incite has been held in other contexts to mean "... [to] urge someone to do something, "[31] The "something" in this case must be an act likely to lead to a breach of the peach. *R. v. Buzzanga and Durocher* may even suggest that the act must lead to an *immediate* breach of the peace. In considering s. 319(2), the court noted that the statements proscribed by subsection (2) -

> ... are not confined to statements communicated in a public place in circumstances likely to lead to a breach of the peace and, consequently, do not pose such an *immediate threat* to public order as those falling under [s. 319(1)] ...[32] (emphasis added)

This appears to set a high standard with respect to Internet communications, as it is difficult to think of a situation where a person reading or viewing a message on the computer screen is motivated to commit a breach of the peace let alone an immediate breach of the peace..

(v) Intent Requirement:

Unlike s. 319(2) , section 319(1) contains no express requirement that the incitement of hatred be willful. However, provisions that do not stipulate a level of intent are assumed to require subjective *mens rea*.[33] Subjective mens rea includes instances when the offence is committed knowingly, recklessly[34] or as a result of wilful blindness.[35] This means that the Crown will need to show that persons inciting hatred did so knowing that it was likely to lead to a breach of the peace or that they were reckless or willfully blind to the consequences of their statement. Reading the intent requirement together with the meaning of incite suggests that it would be difficult to convict a third party that merely facilitates or transmits the hateful statements, unless they were wilfully blind or reckless to the incitement of hatred.

---

[31] *Dionne*, supra note 5.

[32] *R. v. Buzzanga and Durocher*, supra note 8.

[33] *R.. V. Sault Ste. Marie* (1978) 40 C.C.C. (2d) 353 (S.C.C.)

[34] *R. V. Buzzanger, supra note 8*

[35] *R.V. Buzzanga, supra note 8*

In summary, it is probable that s. 319(1) applies to many Internet communications. While the party actually making the statement would likely be liable, liability is less likely for third parties who simply facilitate[36] or transmit[37] the communication, particularly if they are unaware of the specific nature of such activities.

Criminal Code, s. 319(2)

Section 319(2) is concerned with "communicating statements other than in private conversation." The following elements are required to be present for a criminal act to have occurred under s. 319(2).

(i) "Communicating" and "Statements":

Since "communicating" and "statements" are defined in s. 319(7) for the purposes of both subsection (1) and subsection (2), the issues raised by their application to Internet communications in the context of subsection (2) will be the same as those raised in the discussion on subsection 319 (1).

(ii) "Other than in private conversation":

In contrast to the "public place" element required is s. 319(1), the language s. 319(2) is broader since it applies to all statements "other than in private conversation." Although "private conversation" is not expressly defined anywhere in the *Criminal Code*, cases relating to the section dealing with the interception of private communications provide a definition of "private communication" which may be of some guidance.[38] The difference between private communication and private conversation was considered by the Supreme Court of Canada in *R. v. Goldman*:[39]

> The provisions of Part IV.1 of the *Criminal Code* apply to a "private communication" rather than a private "conversation." The difference between the word "conversation" and the word "communication" is significant. A communication involves the passing of thoughts, ideas,

[36] Examples of third parties who facilitate communications would include the operators and moderators of newsgroups, bulletin boards and mailing lists.

[37] Examples of third parties who transmit the communication would include access providers, telecommunication providers and online services.

[38] *Criminal Code*, s. 183.

[39] *R. v. Goldman*, [1980] S.C.R. 976.

> words or information from one person to another whereas "conversation" is a broader term and would include an interchange of a series of separate communications.

Goldman suggests that conversation is a broader term that will likely consist of several communications. The Supreme Court of Canada's statement in *R. v. Keegstra*, uses "communication" and "conversation" interchangeably:

> The fact that s. 319(2) excludes private conversation suggests that the expression of hatred in a place accessible to the public is not prohibited. Therefore, a *conversation or communication* intended to be private does not satisfy the requirements of s. 319(2) if through accident or negligence a person's expression of hatred for an identifiable group is made public. [emphasis added][40]

Goldman and *Keegstra* suggest that we can look to the meaning of "private communication" to determine what might be excluded from s. 319(2) on the basis of being a subset of "private conversation."

"Private communication" has been interpreted by the courts as a communication in which the sender has a reasonable expectation of privacy. This issue is often considered in the context of an alleged breach of s. 8 of the *Canadian Charter of Rights and Freedom*, which deals with unreasonable search and seizure. The Ontario Court of Appeal held that:

> [t]he right of security from unreasonable search arises only in circumstances where there is a reasonable expectation of privacy. A dwelling, an office, an automobile or a briefcase are good examples. But open conversations are not protected because to expect that privacy surrounds them is not reasonable.[41]

---

[40] *Keegstra*, supra note 1.

[41] *R. v. Wong* (1987), 34 C.C.C. (3d) 51 at p. 53.

On this basis, a private communication has been held to include a telephone call[42] but not a computer pager message or a message left at a computer message center, since the pager message could be overheard by people on the street.[43]

There are conflicting authorities on whether a letter is a private communication. On the one hand, the British Columbia Supreme Court held that:

> [W]hen someone sends a letter to another he may hope its contents will not be revealed to a third person, but it would be unreasonable for him as a reasonable person to expect it would not be read by others at any time. He knows or should know the recipient might *voluntarily show the letter to others, or it might get misplaced and come into the hands of a third party* ... Unlike a letter, a telephone call or private discussion is *not given to others for the purposes of transmission nor* is *it intended by the originator that the words be preserved for later reference.*[44] [emphasis added]

On the other hand, a Newfoundland District Court judge has held:

> The search and seizure of private mail is in my opinion a most serious matter. The privacy of one's mail is a most important and highly-protected element of our society. Should it then be less protected than our right to make communication with another by using the telephone? If I write a letter to someone and post it, should it be less protected than if I use the telephone for that purpose? ...It is my opinion that a person's private mail should not be searched or seized without authorization ...[45]

While Canadian courts have not yet considered the nature of Internet communications, the U.S. Military Court of Appeal considered the privacy of e-mail during an appeal from a conviction for distributing child pornography.[46] Though the issue was whether the search of the defendant's e-mail messages violated his Fourth Amendment rights, the analysis applied by the court is similar

---

[42] *R. v. Dunn* (1975), 28 C.C.C. (2d) 538 (N.S. Co. Ct.).

[43] The court held that since pager messages could be overheard by people on the street, there could not be a reasonable expectation of privacy surrounding the conversation: *R. v. Lubovac* (1989), 52 C.C.C. (3d) 551 (Alta. C.A.).

[44] *Regina v. Newall et al (No. 3)* (1982), 69 C.C.C. (2d) 284 (B.C.S.C.)

[45] *R. v. Crane* (1985), 45 C.R. (3d) 368 (Nfld. D. Ct.)

[46] *United States v. Marshall, 42 M.J. 568 (C.M.A., 1995)*

to that in Canadian cases dealing with the interception of private communications.[47]

At trial, the military judge's ruling (later overturned) was that there was no expectation of privacy because:

> ... (1) the e-mail could not be recalled or erased once it was dispatched and the sender was powerless to keep it from being forwarded; (2) the e-mail messages were transferred to screen names rather than to known individuals; and (3) the forwarding of messages to multiple individuals made the situation analogous to bulk mail.

He concluded that the accused was seeking anonymity rather than privacy when he sent the e-mail messages to other users.

The Military Court of Appeal overturned the judge's finding and held that, while the accused may have forfeited his right to privacy to any e-mail transmissions that were downloaded from the computer by another subscriber or removed by a private individual from the online service, he nevertheless maintained an expectation of privacy in any e-mail transmissions as long as they were stored on the online service's computers. The court held that the accused:

... clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that [the accused's] computer transmissions would be received by anyone other than the intended recipients.[48]

While it is unclear how this issue would be decided in a Canadian court, both the trial and appeal judgments indicate the types of factors that a court may consider in determining whether Internet e-mail is a private communication

---

[47] The court applied a two-pronged test to determine whether: (1) the accused had an actual (subjective) expectation of privacy; and (2) the accused's expectation of privacy is one which society believes is reasonable: *Marshall*, supra note 46.

[48] The court referred to *United States* v. *Parrillo*, 34 M.J. 112 (C.M.A. 1992); *United States v. Sturdivant*, 13 M.J. 323 (C.M.A. 1982); and *United States* v. *Sullivan*, 38 M.J. 746 (A.C.M.R. 1993).

It is possible, on the basis of these cases, to make some tentative predictions. The cases suggest that a person posting messages to a Web site, newsgroup, bulletin board or open mailing list would likely not have a reasonable expectation of privacy in their contents, as they will be read by any number of people. Thus, these communications are likely covered by s. 319(2).

In contrast the status of a message communicated through e-mail, a closed mailing list, a private bulletin board or a private interactive chat session has a greater prospect of being held to be a private communication or conversation, if the rationale behind the U. S. Military Court of Appeal's judgment in favour of recognizing e-mail as a private communication is accepted. *Marshall* noted that a user can have an expectation of privacy which is lost only after the message is downloaded to another computer or removed by the recipient from the online service.[49] The *Newall* case, is similarly concerned with the recipient's ability to voluntarily show the message to others, as well as the potential for the letter to become misplaced, the retransmission of the message by another party and the sender's intention to create a permanent record.[50] Each of these factors raised by *Newall* can apply equally to e-mail. Analyzed in conjunction with the *Lubovac* case, the fact that e-mail messages may be intercepted or monitored by a number of parties, such as the online service provider and the access provider, may suggest that e-mail messages, (like pager communications), cannot constitute private communications. If the Canadian courts follow the approach taken in *Newall* and *Lubovac*, e-mail messages would not be considered private communications and could thus not be excluded from the application of s. 319(2) on the grounds that they form a "private conversation." On the other hand, if the courts adopt the interpretation in *Marshall*[51] and *Crane*,[52] e-mail may well comprise a private conversation. Encoding the e-mail will strengthen the argument somewhat, for classifying it as a private conversaiton.

Statements communicated through closed mailing lists would involve a similar analysis, though the many-to-many nature of the communication is a strong factor in favour of finding that mailing list messages cannot form the basis of a private conversation. An analysis of postings to bulletin boards, even if private boards, would likely produce a similar conclusion.

---

[49] *Marshall*, supra note 46.

[50] *Newall*, supra note 44.

[51] *Marshall*, supra note 46.

[52] *Crane*, supra note 45.

A private interactive chat session in audio forms appears to be analogous to a telephone call[53] or a private discussion.[54] On the basis of *Dunn* and *Newall*, statements made in a private interactive chat session may be deemed to be a private conversation. Even if these statements were accidentally interpreted by a third party, such as the system operator, they would not be subject to s. 319(2).[55] If the chat session however is carried out in text form, then the *Newall/Lubovac* vs. *Marshall/Crane* analysis, with its corresponding uncertainties, must be undertaken.

In summary, s. 319(2) appears to apply to messages communicated through Web sites, newsgroups, mailing lists, bulletin boards. There is some prospect that it will also apply to unencoded e-mail, though it may not be applicable to messages communicated through a private interactive audio chat session.

(iii) "Willfully promotes hatred":

While s. 319(1) omits an express reference to the "intent" element, s. 319(2) only applies to persons who "willfully promote hatred." "Willfully" requires that the accused both intend and foresee that his statements will result in the certain stimulation of hatred.[56] It is not enough for the Crown to show that the accused was reckless or was merely aware of the risk of promoting hatred.[57] "Promotes" involves the active support or instigation of hatred; a simple encouragement or advancement of hatred is insufficient.[58] This s. 319(2) may set a higher standard with respect to Internet communications than does s. 319(1). While s. 319(2) may apply to persons posting messages with the intention of instigating hatred, it does not appear applicable to third parties who merely provide the means or facilities for communicating the message, even if they are aware of the contents. At most, third parties who are aware of the contents of the hate messages (and even supportive

---

[53] *Dunn*, supra note 42.

[54] *Newall*, supra note 44.

[55] *Keegstra*, supra note 1.

[56] *Keegstra*, supra note 1.

[57] *Keegstra*, supra note 1.

[58] *Keegstra*, supra note 1.

or encouraging of them), may be said to be aware of the risks of promoting hatred, but according to *Keegstra*, this is not enough to convict under s. 319(2).

Criminal Code, s. 320

Section 320 permits the seizure and forfeiture of copies of publications believed to be hate propaganda when the copies are kept for distribution or sale. "Hate propaganda" is defined broadly as "any writing, sign or visible representation that advocates or promotes genocide or the communication of which ... would constitute an offence under section 319."[59] It is likely that this definition, by including the statements prohibited by s. 319, would encompass files on CD-ROM, computer disks or even on a computer hard drive.[60] Thus, s. 320 may permit the seizure and forfeiture of any CD-ROMs, disks or even hard drives as long as they are being used for the distribution of what is believed to be hate propaganda. However, the application of this section to allow seizure of such couputer equipment may be greatly limited, if a defence can be made to the effect that the disks, hard drive etc., are themselves not going to be distributed, but are only used as storage devices for a file whose electronical embodiment will be distributed.

Canadian Human Rights Legislation

Section 13(1) of the *Canadian Human Rights Act* has been used successfully to prosecute the Western Guard Party and the Church of Jesus Christ-Aryan Nations for racist telephone messages. Although the Act's provisions were intended to target the dissemination of hatred through telephone answering machines, they appear to be broad enough to include any Internet communications transmitted through a telecommunication facility, as most users connect to the Internet through a computer, telephone line and modem. While subsection (3) makes it clear that the owners and operators of the telecommunication facilities will not be liable when their facilities are merely used to transmit the message, it is unclear whether newsgroup, BBS or mailing list operators or moderators, who play a more active role, would be similarly exempted.

The convergence of Canadian telephone and broadcasting industries may make the application of s.13(1) somewhat less certain in the future, as subsection (2) creates an exemption for any message transmitted in whole or in part by a broadcasting facility. Furthermore, the current ability to communicate multi-media messages on the Internet, consisting of sound, text and even video, has the potential of making every Internet user a "broadcaster" and further blurring the distinction between telecommunication and broadcasting. While an analysis of the appropriate regulatory scheme is beyond the scope of this study, the following discussion will assume that users, information providers and

---

[59] *Criminal Code*, s. 320(7).

[60] See the discussion of "communicating" and "statements" with respect to section 319(1) above.

access providers may have potential liability for disseminating hate messages under s. 13(1) of the *Canadian Human Rights Act*.

Broadcasting Act

Because most Internet communications currently consist of alphanumeric text, these communications would likely not comprise "broadcasting" which is subject to the *Broadcasting Act*.[61] However, information providers such as the C.B.C. are increasingly posting "broadcasts" of original programming on the Internet, capable of being viewed, listened to or downloaded by users at their leisure. With the advent of the World Wide Web and the facilities it provides for transmitting graphics, audio and video, it may well be that it is the *Broadcasting Act* that would have some application to such multi-media communication. While a detailed analysis of the applicability of the *Broadcasting Act* to Internet communications is beyond the scope of this report, the discussion below will leave open the possibility that, multi-media communications posted to the Internet, particularly by a CRTC licensee, may create a liability under the *Broadcasting Act*, if they are likely to expose an individual, group or class of individuals to hatred or contempt on the basis of a discriminatory ground.[62]

[61] Section 2(1) of the Broadcasting Act defines broadcasting as "*...any transmission of programs.*" "*Programs*" is defined as "*...sounds or visual images ;;; [not including] visual images, whether or not combined with sounds, that consist predominantly of alphanumeric text.*"

[62] See note 20.

II. ACTIVITIES AT RISK

1. A party Creates and Communicates a Hate Message Through a Web Site, Newsgroup, BBS, Mailing List, E-Mail or Interactive Chat Session.

Issue

A party communicates a hate message via a Web site, newsgroup, mailing list, bulletin board, e-mail or interactive chat session.

Discussion of Liability:

Liability of the party who actually makes the statement (whether genocide or hatred) will likely not be affected by the party's role in the Internet chain. For example, a BBS subscriber will face the same liability as a BBS operator, as long as each was the originator of the hate message.[63]

(i) ***Criminal Code*, s. 318:**

The party making the statement may be liable for advocating and promoting genocide over the Internet under s. 318, provided the statement is deemed to be active encouragement rather than a mere communication of opinion.

(ii) ***Criminal Code*, s. 319(1):**

A party may be liable for inciting hatred over the Internet, which is likely to lead to a breach of the peace under s. 319(1). To convict under this section, the Crown will have to prove that the party incited hatred knowingly, or was reckless to the potential consequences of the statement i.e. likely to lead to a breach of the peace.

A party charged under s. 319(1) could raise a defence in a number of ways. First, it could challenge the assertion that the message was communicated in a "public place," noting that the message was communicated through a computer and modem in the user's own home. However, as discussed previously, the courts would likely hold that by posting the message to a medium which many, if not all, members of the public may access and read, the user was "in view of the public" and thus in a public place for the purposes of s. 319(1).[64] If the message was

---

[63] On the other hand, the liability of a BBS operator will likely be different if the statement is posted by another person.

[64] *McEwen, Figluizzi, Wise* and *Smith*, supra note 30.

communicated through private e-mail, the party who communicated the message may be in stronger position to support the defence that e-mail is not a public place to which members of the public have access, since an individual e-mail account, unlike other Internet applications, is generally for the use of only one subscriber. This would be a particularly strong argument if the message was encoded.

Second, the party could suggest that although he communicated the statement, this was done merely to express an opinion or encourage a discussion, rather than with the intent to incite hatred. Even if the court accepts this argument, it may nevertheless convict the party on the basis of recklessness or willful blindness. Such a defence is very much fact dependent.

Finally, and as the strongest defence, the party could point out that s. 319(1) is meant to target incidents that pose a threat (perhaps an immediate threat) to public order.[65] Although the success of this defence is fact dependent, it would be difficult to visualize circumstances where a message read on a computer screen, even though inciting anger or hatred, would encourage the reader to actually commit a breach of the peace, particularly an immediate breach.

(iii) *Criminal Code*, s. 319(2):

The party making the statement may be liable for willfully promoting hatred under s. 319(2), depending on the manner in which the statement was communicated (i.e. not private conversation). The Crown would also need to prove beyond a reasonable doubt that the party making the statement both intended and foresaw that the statement will result in the stimulation of hatred.[66] The party's actions would need to amount to active support and instigation of hatred; it would not be enough for the Crown to show that the accused was reckless or was merely aware of the risk.

A party charged under s. 319(2) could present a defence on several grounds. It could suggest that while it foresaw that the statement may result in the promotion of hatred, this was not the user's intention in making the statement (i.e. not wilful).

Furthermore, while the stimulation of hatred may have been a possible consequence of the user's statements, it was not a certainty or even foreseeable as likely.

---

[65] *Buzzanga and Durocher*, supra note 8.

[66] *Keegstra*, supra note 1.

A strong defence could be raised as a result of the medium used to communicate the statement. The user could challenge the application of s. 319(2) on the basis that the statement was part of a private communication. This argument would likely be most effective for messages communicated through e-mail, private bulletin boards, closed mailing lists and private interactive chat sessions. The Canadian courts have not yet addressed the nature of these communications and it is difficult to predict the effectiveness of such a defence. For a discussion of the factors and case law that a court may consider in deciding whether such communications comprise a private communication, see the discussion above.

(iv) *Criminal Code*, s. 320:

If the party keeps copies of the hate message on disk or a computer hard drive for the purpose of posting them to the Internet or transmitting them through e-mail, the disk and the hard drive may potentially be seized and ordered forfeited, if the hate messages are believed to be hate propaganda.[67] It will be interesting to learn if the courts accept the defence that these components of equipment were not themselves going to be physically distributed, and therefore are not subject to seizure.

(v) Federal Human Rights Acts:

If the communication was made repeatedly, the party making the statement may be liable for contravening s. 13 of the *Canadian Human Rights Act*. Although a detailed analysis of provincial legislation is beyond the scope of this study, it is likely that the user may also be liable under the anti-discrimination provisions of Provincial human rights acts, for exposing a person or group of persons to hatred on the basis of the prohibited grounds of discrimination.

(vi) Broadcasting Act

The relevant *Broadcasting Act* regulations, if applicable at all to Internet communications, would only prohibit *licensees* from distributing hate messages in their programming. Furthermore, the Act's definition of "program" specifically excludes visual images that consist predominantly of alphanumeric texts. On this basis, the *Broadcasting Act* prohibitions against hate messages would likely not apply to the majority of Internet users. On the other hand, if the party making the statement was, for example, a licensee such as the C.B.C., and the statement was communicated through the Internet, by sounds or visual images in the form of a

[67] See section I, above.

sound, video or multimedia file posted to the Internet, the party may indeed face liability for contravening the Act.

Relevant Legislation:

Criminal Code, ss. 318, 319(1), 319(2) and 320
Canadian Human Rights Act, subsections 13(1) and (3)
Provincial Human Rights Acts
Broadcasting Act Regulations

Self-Aide Practices:

A party could minimize its risk for transmitting content which could be characterized as hate messages by:

(i) educating itself on what constitutes hate propaganda; and

(ii) assessing each message before posting to ensure that it does not advocate, promote or incite hatred or genocide against an identifiable group.

2. A Third Party Facilitates or Transmits a Hate Message Created and Communicated by one of its Users.

Issue:

A party ("Facilitator") may face liability for facilitating the sending, or simply transmitting, a hate message created and communicated by one of its users, visitors or subscribers. Examples of such facilitators include telcos, Internet access providers, online services, BBS, newsgroup or mailing list operators and BBS, newsgroup or mailing list moderators. The following discussion will differentiate between two types of facilitators: (1) those who are either unaware of the hate messages, or are aware of the messages but do not intend to advocate, promote or incite hatred or genocide ("group one"); and (2) those who administer services for the specific purpose of facilitating hate messages ("group two"). Most access providers, for example, would fall into the first group. A member of a hate group who sets up a bulletin board as a forum for the exchange of hate literature would fall into group two.

Discussion of Liability:

(i) *Criminal Code*, s. 318:

While s. 318 does not explicitly preclude its applicability to facilitators, the requirement that the person charged "advocate or promote" genocide would likely make it difficult to convict a facilitator that is merely providing a means or facilities for transmitting the hate message. "Promote" has been held to require active encouragement.[68] On this basis, third parties falling into group one would likely not be liable under s. 318. With respect to group two, the action of setting up a newsgroup, mailing list or bulletin board specifically for the purpose of disseminating hate literature may make the operator and/or moderator liable even if the message was actually posted by another person. Such group two types of activities seem to show more clearly an invention to advocate or promote genocide, which exceeds simple support or encouragement.

Liability for either group may also depend on the amount of control the facilitator exercises over its users' messages. The operator or moderator of a general purpose newsgroup, for example, may be deemed to exercise sufficient control over the newsgroup's contents to make him seem to be "responsible", at least morally, for any hate messages which he permits to be posted. Whether or not the failure to delete such content is enough to constitute the higher standard of actively supporting the advocating and promoting of hatred, however, is uncertain. Certainly there is a greater risk for inaction by a facilitator in such circumstances.

(ii) *Criminal Code*, s. 319(1):

Since the definition of "communicating" appears not to be limited to those who actually make the statement, a third party facilitating or transmitting the hate message could be deemed to be communicating it, which would be sufficient for the purpose of s. 319(1). Liability under s. 319(1) will depend on whether the Crown can prove that the facilitator knowingly, recklessly or through wilful blindness, incited hatred likely to lead to a breach of the peace. Whether a facilitator that was simply aware of or had reason to believe that hate messages were being posted to or transmitted by its facilities without specifically knowing or believing that the messages could lead to a breach of the peace, would be liable under s. 319(1) is unclear.

Incite has been held to mean "to urge someone to do something", and the "something" in this context must be to create hatred in a third party 's mind that will likely lead to a breach of the peace. On this basis, it would be difficult to show

[68] *Keegstra*, supra note 1.

that the third parties falling into group one were themselves actually urging a breach of the peace, simply by transmitting the hate messages. On the other hand, it could be argued that a facilitator that actively administers a forum for the exchange of hate literature may be deemed to be inciting hatred through its active role in facilitating the exchange of hate messages.

A third party charged under s. 319(1) could back its defence on several grounds. First, it could challenge the interpretation of "communicating" by suggesting that it implies an active role and must thus be limited to the person actually making the statement. Based on the plain language of the provision, it seems that this is a relatively weak defence.

Second, it could challenge the assertion that the message was communicated in a "public place" by: (1) noting that its facilities are privately owned; or (2) suggesting that "public place" was intended to apply to physical locations rather than a "virtual" place. If the courts rely on decisions in other contexts, it seems likely that the courts will give a broad interpretation to "public place" as encompassing all Internet communications (except perhaps private e-mail).

Finally, the party could point out that s. 319(1) is meant to target incidents that pose a threat (perhaps even an "immediate threat") to public order and suggest that while a message read on a computer screen may incite anger or even hatred, it is unlikely that the message will encourage the reader to commit a breach of the peace. This seems to be a strong defence, although ultimately dependent on the factual situation.[69]

(iii) *Criminal Code*, s. 319(2):

A facilitator will only be liable for hate messages under s. 319(2) if the facilitation or transmission of the hate message is deemed to constitute the "wilful" promotion of hatred. A facilitator, such as in group one who was unaware of the hate message or was at most reckless or willfully blind, would not appear to be liable under this section. Even if the third party was aware of the message, it would in many cases be difficult for the Crown to prove beyond a reasonable doubt that such facilitator both intended and foresaw that facilitating or transmitting the message would result in the certain stimulation of hatred.[70]

---

[69] *Buzzanga and Durocher*, supra note 8.

[70] *Keegstra*, supra note 1.

A facilitator charged with s. 319(2) could defend liability on several grounds. First, it could suggest that while it foresaw that facilitating or transmitting the statement could potentially result in the stimulation of hatred, it was not the third party's intention that it do so.

Second, it could concede that while the stimulation of hatred may have been a possible consequence of facilitating or transmitting the statements, it was not a virtual certainty.

Also, depending on the manner of communicating the statement, the third party could challenge the application of s. 319(2) on the basis that the statement was part of a "private conversation". This argument would likely be strongest for messages communicated through private bulletin boards, closed mailing lists and private interactive chat sessions, and particularly encoded e-mail. Since the Canadian courts have not yet addressed the nature of these types of communications, it is difficult to predict the effectiveness of such a defense. For a discussion of the factors and case law that a court may consider in deciding whether such communications comprise a private communication, see the discussion in Part I.

(iv) *Criminal Code*, s. 320:

If the facilitator's server makes copies of the messages transmitted by its users, the hard drives could potentially be seized and ordered forfeited if the users' hate messages are believed to be hate propaganda and the third party's transmission of the messages is deemed to be distribution. A seemingly strong defence against such seizure is based on the fact that the hardware components are not publications which themselves would be distributed.

(v) Federal Human Rights Acts:

If the communication was made repeatedly, the third party may be liable for contravening s. 13(1) of the *Canadian Human Rights Act*. The third party could seek to escape liability by relying on the s. 13(3) exemption for the owners or operators of telecommunication facilities in the applicable circumstances. Whether the *Canadian Human Rights Act* will not be interpreted as strictly as the *Criminal Code* to extend the benefit of the s.13(3) exemption to access providers and other third parties that merely facilitate or transmit the communications, is unclear.

Although a detailed analysis of provincial legislation is beyond the scope of this study, it seems possible that the facilitator may also be liable under the anti-discrimination provisions of provincial human rights acts for exposing a person or group of persons to hatred on the basis of a prohibited ground of discrimination.

Similar factors varying the prospect of liability and successful defence, as found in the Criminal Code sections, would likely be relevant.

(vi) ***Broadcasting Act***

The relevant *Broadcasting Act* regulations, if applicable at all to Internet communications, would seem only to prohibit *licensees* from distributing hate messages in their programming. Furthermore, the Act's definition of "program" specifically excludes visual images that consist predominantly of alphanumeric tests. On this basis, the *Broadcasting Act* prohibitions do not appear to apply to third parties facilitating or transmitting hate messages created and communicated by their users.

Relevant Legislation:

Criminal Code, ss. 318, 319(1), 319(2) and 320
Canadian Human Rights Act, subsections 13(1) and (3)
Provincial human rights acts
Broadcasting Act Regulations

Self-Aide Practices:

A facilitator may be able to minimize its liability by taking one or more of the following steps;

(i) educating itself on what constitutes hate propaganda;

(ii) adopting a procedure for screening online content;

(iii) adopting an "Acceptable Use Policy" that: (a) expressly forbids the posting or exchange of hate propaganda or other illegal materials; and (b) requires its users to immediately notify the facilitator of any illegal content found on the system;

(iv) adopting a procedure for responding actively to illegal content. For example, upon becoming aware that particular materials may constitute hate propaganda, the provider could immediately assess the content and request a withdrawal by the party posting, and if necessary delete the materials from its system. This could be made subject to "clearance" obtained by the posting party from law enforcement officials;

(v) posting warnings of potentially offensive content;

(vi) developing a procedure for dealing with complaints from users or other parties about offensive material.

Such steps, at the least, will help the third party challenge the Crown's assertion of recklessness or willful blindness for the purpose of s. 319(1).

3. A Party Posts a Hate Message to a Foreign Server

Issue:

A Canadian posts a hate message to a server located in a foreign jurisdiction.

Discussion of Liability:

Liability in this situation is uncertain, as it is unclear whether or where the offence is actually committed. The *Criminal Code* is jurisdictional in nature and virtually never applies to acts taking place outside Canada's territory, except in some very limited circumstances such as the transportation field. Due to the "virtual" nature of the Internet the site of the offence is unclear.

(i) *Criminal Code*, s. 318 and s. 319(2):

If it is the act of *posting* that actually comprises the offence, regardless of the location to which it is posted, then the party making the statement could potentially be liable for advocating and promoting genocide under s. 318 or for willfully inciting hatred under s. 319(2). Similarly a third party, located in Canada, who facilitates or transmits the hate message could also be liable, subject to the exceptions discussed above.

(ii) *Criminal Code*, s. 319(1):

With respect to s. 319(1), the court will need to clarify what is meant by a "public place." If "public place" is intended to focus on the *physical place* where the message is stored, neither the person making the statement, nor the foreign party on whose server the message resides, may be liable under the s. 319(1) of the *Criminal Code*. If, on the other hand, the focus is on the Canadian *public*, the courts may apply the *Lavoie* principles to suggest that the party making the statement is "in view of the public"[71] and that this is sufficient for the purpose of s. 319(1). The liability of third parties under s. 319(1) is similarly uncertain.

[71] *Lavoie*, supra note 29.

Relevant Legislation:

Criminal Code, ss. 318, 319(1), 319(2).

Self-Aide Practices:

The practices would be similar to those Self-Aide Practices discussed in the section above.

[Cat. N.: C2-312/1997E ISBN: 0-662-25489-9]

TRADE-MARKS

I. PROHIBITED CONDUCT

1. Overview of Applicable Law on Trade-Marks

There are three major provisions in the Canadian Trade-Marks Act that deal with the unauthorized use of trade-marks. These sections, 19, 20, and 22 depend in large part on the meaning of "use" set out in section 4.

Trade-Marks Act, s. 4:

> Section 4 outlines when a trade-mark is deemed to be in use for the purposes of the *Trade-marks Act*, including unauthorized or infringing use. The use definition depends on whether the trade-mark is used in relation to a product or a service.
>
> A trade-mark in relation to goods is deemed to be used if, at the time the title to or possession of the goods is transferred, the trade-mark is: (a) marked on the goods; (b) marked on the packages in which they are distributed; or (c) associated with the goods in a way that gives notice of the association to the person to whom the property possession is transferred.[1]
>
> A trade-mark in relation to services is deemed to be used if it is used or displayed in the performance or advertising of those services.[2]

Trade-Marks Act, s. 19

> Section 19 gives the owner of a registered trade-mark the exclusive right to use that exact trade-mark in relation to those goods or services for which it is registered. The exclusive right only applies to use throughout Canada.[3]

---

[1] *Trade-Marks Act*, s. 4(1).

[2] *Trade-Marks Act*, s. 4(2).

[3] *Trade-Marks Act*, s. 19.

Trade-Marks Act, s. 20

Section 20 deals with confusingly similar trade-marks or trade names. It states that using a confusing trade-mark or trade name in relation to the sale, distribution or advertising of any goods or services infringes a registered trade-mark owner's right to its exclusive use. The section outlines three exceptions in which use of a confusingly similar trade-mark is permitted, provided it does not depreciate the trade-mark's goodwill: (a) any bona fide use of a personal name as a trade name; (b) any bona fide use, other than as a trade-mark, of the geographical name of a place of business; or (c) any bona fide use, other than as a trade-mark, of any accurate description of the character or quality of goods or services.

Trade-Marks Act, s. 22

Section 22 prohibits the use of a trade-mark registered to another person in a way that is likely to depreciate the trade-mark's goodwill. This provision however is not as broad in its application as the U.S. *Federal Trademark Dilution Act of 1995.*

2. Application to Internet Activities

Meeting "Use" Requirements

The technical use requirements as defined by s. 4 of the Act are particularly important in establishing infringement under s. 19 or a depreciation of goodwill under s. 22. While this may not be difficult to do in normal commerce for goods or services, when it comes to business on the Internet, only use of the trade-mark in relation to services is easily proven. In order to show use of a trade-mark in respect of any services, all that is required under s.4(2) is its incorporation in the advertising of the services.

Satisfying use requirements for trade-marks in relation to commerce dealing with goods is more challenging on the Internet. Section 4(1) requires that trade-marks used in relation to goods appear on the goods or their packaging or are otherwise associated with the goods, *at the time of the transfer of their title or their possession*. Incorporation of a trademark into advertising of goods is not sufficient to constitute use. Since the trade-mark use requirements in s. 4(1) must coincide with the time of transfer of title or possession of the goods, it is unlikely that any appearance of the trade-mark on the Internet will constitute "use" for the many goods of a tangible nature which are delivered subsequently through non-Internet facilities. There are two possible exceptions.

First, it may be possible for a trade-mark which appears on digital based goods, such as software, videos or music files to constitute use, even if the goods are delivered solely through the Internet. This results from the definition of use for goods, which includes the association of a trade-mark with products at the time that their "possession" passes to the new owner. Such a proposition seems to have been indirectly accepted in both Canada and the U.S. In Canada, the Federal Court held that a trade-mark used as an access code to retrieve software constituted "use" under the Act, since it appeared on the screen at the time of the retrieval.[4] Similarly, the U.S. Trade-marks Office has accepted a printout showing how a trade-mark appeared on the computer screen during transmission, as evidence of "use".[5]

Second, depending on whether courts recognize the validity of electronic contracts, it may be possible to transfer title to tangible goods solely on the basis

---

[4] *BMB Compuscience Canada Ltd v. Bramalea Ltd.*(1989) 22 C.P.R. (3d) 561 (F.C.T.D.).

[5] *In Re Metriplex Inc.* 23 U.S.P.Q. 2d 1315 (T.T.A.B. 1992).

of an electronic contract entered into and concluded on the Internet without any other documents. A trade-mark appearing on such an electronic contract could thereby constitutes "use" in conjunction with transfer of title.

Direct Infringement vs. Vicarious Liability, Contributory Infringement and Conspiracy

Direct infringement is committed by a party itself using a mark that infringes a registered mark or depreciates the goodwill of a third party's trade-mark. Thus, any person posting or supplying content to the Internet containing a third party's mark will likely be liable for direct infringement under sections 19, 20 or 22 of the Act.

It is unclear whether other parties, who merely facilitate the posting or transmission of the infringing mark, may also be liable for direct infringement. The possibility that these parties may be deemed vicariously liable or liable for contributory infringement is more likely but still uncertain at this time in Canadian law, due to the absence of relevant cases. This issue was recently argued in a case in Virginia, involving the domain name administrator as a defendant on the basis of contributory infringement. There is also a possibility of liability for "conspiracy to infringe" occurring if the facts bear out such a deliberate joint agreement to infringe.[6]

[6] *Porsche Cars North America Inc. v. Chen, No. 96-1006-A* (E.D. Va., filed July 26, 1996): *Pizza Pizza Ltd. v. 528635 Ontario Inc.* (1987) 16 C.P.R. 186 (Ont HC)

II. ACTIVITIES AT RISK

1. Content Provider Supplies Through Its Own Facilities, Content Infringing a Third Party's Trade-mark

Trade-mark infringement on the Internet normally will take one of two forms: "traditional" infringement, through the use of a third party' mark or a confusingly similar mark and infringement of a third party's trade-mark through the use of a domain name that includes the trade-mark or a similar mark.

Issue

An information provider supplies content through its own internal facilities e.g. Web site or on-line information service. The content contains a mark that either infringes, or depreciates the value of, a third party's trade-mark. The reduction of goodwill may be caused by the site's disparaging comments about the third party, its goods or its services, or by creating an inappropriate association between the information provider, or its site, and the third party, its goods or its services

Parties Potentially Liable

(i) Information provider:

If the information provider's content contains a mark identical to the third party's trade-mark and the information provider's use relates to goods or services, the information provider may be liable for infringing the trade-mark owner's rights under s. 19. of the *Trade-Marks Act.* Liability will be more certain if the mark usage is with respect to services (as opposed to goods) or with digital based goods supplied over the Internet. The difference in potential liability arises due to the different definitions in section 4 of the *Trade-Marks Act* of what constitutes use of a trademark for goods as opposed to services.

If the information provider's content contains a mark not identical but merely confusingly similar to the third party's trade name or trade-mark, the information provider may under s. 20 still be liable for infringement if the provider is in the business of selling, distributing or advertising goods or services. It is not necessary that the goods or services associated with the infringing mark be the same as the goods or services associated with the third party's trade-mark. The information provider's use of a mark (or trade name) in relation to *any* goods and services may be enough to create

liability under s. 20 if such use causes confusion with the trade-mark of the third party. The issue of goods vs. services being promoted, and the type of goods, will have an impact on the likelihood of liability (see discussion above).

If the use of the mark in the content depreciates the goodwill of the third party's trade-mark, the information provider may also be liable under s. 22 of the Act, even if the information provider is not in the business of selling goods and services. Whether the mark depreciates goodwill is determined based upon the facts of each case relating to type of activity being undertaken by the information provider.

Although there are still no Canadian cases on these points, several decisions in comparable cases in the United States have been handed down or are in the process of being awarded.[7]

(ii) Access provider:

If there is a separate Internet services access provider who operates a web site and/or provides Internet access to the information provider, the access provider may theoretically be liable for contributory infringement or conspiracy to infringe. Although no cases to date have addressed this issue in Canada, there is implied in several trade-mark decisions a requirement that a deliberate appropriation of the mark, or a wilful and knowing participation in the act, occur in order for liability to be imposed.[8] It is likely that in most cases the access provider will not have such an involvement.

Relevant Legislation

Trade-Marks Act, ss. 4, 19, 20 and 22

---

[7] *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D.Fla. 1993): *Sega Entertainment, Ltd. v. MAPHIA*, 857 F. Supp. 679 (N.D.Cal. 1994): *Hasbro v. Internet Entertainment Group*, C96-130WD (W.D. Wash. 1996): *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*, 1996 U.S. Dist. LEXIS 8435

[8] *Pizza Pizza, supra note 6; Lee's Food Products Ltd. v. Shafer - Haggart Ltd.* (1984), 81C.P.R. (2d) 204; K-Tel International Ltd. v. Benoit (1995) 92 F.T.R. 157.

Self-Aide Practices

(i) Information provider could review all content and delete or "clear" any incorporated third party works which contain trade-mark references.

(ii) Access provider could contractually require content provider to review its content before posting, and also obtain an indemnity agreement from the content provider.

(iii) Information provider could incorporate a disclaimer relating to posted material which it has not reviewed

2. Subscriber Posts Content Infringing Someone's Trade-Mark, to a Third Party's Web Site, Newsgroup, BBS or E-Mails Content to Mailing list.

Issue

A subscriber posts content to an unrelated Web site, newsgroup, BBS, or sends E-mail to a mailing list. The content contains a mark that either infringes or depreciates the goodwill of a third party's trade-mark. In this situation, the Internet destination (e.g. web site, BBS) is not controlled, directly or indirectly, by the subscriber.

Parties Potentially Liable

(i) Subscriber:

As in the case above, if the infringing mark is identical to the third party's trade-mark and the subscriber's use constitutes a "use" under the Trade-Marks Act, the subscriber may be liable for infringing the trade-mark owner's rights under s. 19.

Similarity, if the infringing mark is not identical but merely confusingly similar to the third party's trade name or trade-mark, the subscriber may be liable for "deemed infringement" under s. 20, if the subscriber is in the business of selling goods and services.

And if the subscriber depreciates the goodwill of the third party's trade-mark, the subscriber may be liable under s. 22 of the Act.

(ii) Newsgroup, BBS or mailing list operator:

The newsgroup operator could theoretically be held liable for the infringement, through contributory infringement or conspiracy theories. This would appear likely if the content posted to the newsgroup or BBS, or sent to a mailing list, is screened (or is supposed to be screened) by a submission moderator.

(iii) Submission moderator:

The submission moderator could theoretically be held contributorily or vicariously liable for the infringement, if the moderator reviewed the content, identified the use of an infringing mark and failed to take any action

(iv) Access provider:

The access provider may also in theory be held vicariously or contributorily liable for the infringement, but this is likely only in the event that it had clear prior knowledge of the unauthorized use of the infringing mark.

Relevant Legislation

Trade-Marks Act, ss. 4, 19, 20 and 22

Self-Aide Practices

(i) Subscriber could review content and delete or "clear" any incorporated third party marks.

(ii) Newsgroup, BBS or mailing list operator could contractually require the subscriber to review its content before posting, and also obtain an indemnity agreement. Use of a submission moderator to screen infringing material could potentially reduce liability, if active steps are taken to delete or reject any such material which is discovered.

(iii) Operator and access provider could each include a disclaimer as to lack of review for infringing material posted.

3. Web of Internet Site Operator/Owner Facilitates Access to an Infringing Site by Hyperlink

Issue

Consider an Internet site that contains a mark that infringes, or depreciates the goodwill of, a third party's trade-mark. Will a person facilitating access to such an infringing site by establishing a pointer (hyperlink) at another web or other Internet site incur liability?

Parties Potentially Liable

(i) Hyperlink creator/supplier:

There are no cases in Canada that have addressed such a question. However, based on the discussion above, it would be reasonable to assume that a hyperlink supplier that had full knowledge of the infringing content of the linked site and made no effort to at least advise users of such a situation, could in theory be held to be liable for trade-mark infringement. However, unless the hyperlink supplier actually conspired with the infringer, participated in establishing the infringing site, or actively promoted the existence of the infringing site and induced users to visit it, the possibility of being found liable seems somewhat remote.

Relevant Legislation

Trade-Marks Act, *ss* 4, 19, and 20

Self-Aide Practices

The hyperlink supplier could delete the link/pointer if it becomes aware of the infringing activity.

Alternatively, it could consider posting a notice in proximity to the hyperlink, or which comes up on screen where the hyperlink is triggered, advising of its inability to control the content at the hyperlinked site, and the fact that it has not verified the content for accuracy or compliance with legal requirements.

4. Domain Name Conflicts With a Third Party's Trade-Mark

Issue

A party uses a domain name that is identical to, or incorporates, a third party's registered trade-mark.

Parties Potentially Liable

(i) Domain Name holder

Sections, 19, and 20, which deal with marks that are identical or confusingly similar to a registered trade-mark of a third party, require that there be a "use" under the Act for liability to occur. As a result, the domain holder will likely not be liable under these sections, unless the mark is being used not only in its normal role as an address locator, but in a secondary role as a trade-mark.

If the domain name holder uses the domain name for the secondary purpose of selling its services, then the display or advertising of those services on the Internet in association with the domain name could make the owner liable under s. 19.

On the other hand, it would be more difficult to show that a domain name satisfies the use requirements for infringement to occur in relation to goods. The domain name would not appear on the goods themselves, unless they were of a digital nature capable of being transferred over the Internet (together with the domain name).

However the use of the domain name could potentially create liability under s. 22 if it depreciated the goodwill of the third party in its registered trade-mark. It is hard to imagine that goodwill would not be depreciated if the mark was being improperly used to sell goods or services owned by the domain holder. Liability would be somewhat more difficult to prove if the domain name holder was not involved in a commercial activity of selling goods or services.

If the domain name is administered by an organization such as the Internic which allocates the functional domains (e.g. .COM, .EDU, .NET, etc.), the domain name owner may also face non-legal consequences under Internic's domain name policy. Specifically (1) the domain name may be temporarily

put on hold, pending the outcome of legal proceedings, during which time the domain name holder will need to refrain from using the domain name; and (2) the domain name holder may be required to post a bond or sign an indemnity agreement to indemnify Internic against any legal proceedings arising out of the domain name owner's infringement of a third party's trade-mark. Although the Canadian domain registrar has not yet established a policy for disputes over the .CA domain names, there is a real prospect that a similar policy will be adopted in the not too distant future.

Consider the various cases in the United States dealing with this area. Although they have been decided on the basis of different wording in U.S. trademark laws they offer some relevant principles of public policy and legal theory.[9]

Relevant Legislation

Trade-Marks Act, ss 4, 19,20 and 22

Self-Aide Practices

(i) Domain name holder to undertake trade-mark searches in the United States (for the functional domain names) and in Canada (for the .CA domain) prior to requesting a domain name from the domain administrator.

---

[9] *Avon Products v. Carnetta Wong Associates* (E.D.N.Y., filed February 2, 1996): *Comp Examiner Agency v. Juris, Inc.*, No. 96-CV-213 (C.D.Cal., April 26, 1996): *The Hearst Corporation v. Goldberger*, Civil Action No. 96 Civ 3620 (PKL) (S.D.N.Y., filed May, 1996): *Inset Systems, Inc. v. Instruction Set, Inc.*, 1996 U.S. Dist. LEXIS 7160 (D. Conn 1996): *Regis McKenna Inc. v. Regis Corp.*, C-96-20551 (N.D.Cal., filed July 9, 1996): *American Commercial, Inc. v. Sports & Leisure International Inc.*, No., SA CV 96-713-LHM (C.D. Cal., filed July 25, 1996): *Nu Skin International Inc. v. Chen*, Civ. No. 960400538 CN (Utah Dist. Ct., August 28, 1996): *Actmedia v. Active Media International, Inc.*, 1996 WL 466527 (N.D.III. 1996):

5. Domain Name is Confusingly Similar to Another Domain Name

Issue

A party uses a domain name that is confusingly similar to another party's domain name. The domain names differ only with respect to their top level functional (organizational) zones or geographical zones, or else there is only a minor or inconsequential difference in the spelling of the domain name prefix.

Parties Potentially Liable

The domain name holder that will most likely prevail will be the one that has a corresponding registered trade-mark. The liability analysis in this case is the same as in Activity 4 above. If neither domain name holder has any registered trade-mark rights corresponding to its domain name, then priority of rights will be based on prior use as a trade-mark (whether by traditional means or by the domain name if it constitutes use) and liability will likely be more difficult to establish.[10]

Relevant Legislation

Trade-Marks Act, ss. 4, 19, 20, and 22

Self-Aide Practices

(i) Domain name holders to undertake trade-mark searches in the United States (for organizational domain names) and Canada (for .CA domain) prior to requesting a particular domain name.

---

[10] *Nova Star, Inc. v. Impact Technology.*, No. CV 95-13874 (Sup. Ct., Phoenix AZ)

6. Domain Name Diminishes Goodwill of a Third Party's Trade-Mark

Issue

The grant of a top-level domain name (whether organizational or geographic zone) prevents any other person obtaining the same name for the same zone, even for a totally different business or industry. All registered trade-mark owners of this name can suffer "trade-mark dilution" (the depreciation of value of the goodwill in a mark) due to an incompatible or seemingly innocuous use made of the domain name and their inability to use their own trade-marks as a domain name. Even owners of unregistered trademarks can be affected leading to a claim based on confusion and passingoff.[11]

Parties Potentially Liable

If the domain name holder has a registered trade-mark corresponding to its domain name, then it will retain that domain name monopoly even if other parties have registered the exact same trade-mark for different goods or services. The domain name holder will likely not incur any liability to any other registered trade-mark owner for use of the domain name, unless the activities that it carries on under its domain name also evidence a secondary use as a trade-mark for the goods or services for which the other trade-mark owners registered their marks. In such case the analysis would be the same as in Activity 4 above.

Relevant Legislation

Trade-Marks Act, ss.4, 19, 20 and 22

Self-Aide Practices

(i) Domain name holder to undertake trade-name searches to determine what rights third parties have to the same or similar mark or business name, and in which fields of business, and ensure that its activities do not spill over into such areas.

---

[11] *PEINET Inc. v. O'Brien* (1995) 61 C.P.R. (3d) 334 (PEISC)

7. Domain Name Conflicts with Foreign Trade Name or Trade-Mark

Issue

A Canadian party uses a domain name that, while not infringing any trade-mark or trade name rights in Canada, is actually the same as or confusingly similar to a trade name or trade-mark used outside of Canada.

Parties Potentially Liable

Domain Name User:

While no liability would arise in Canada under Canadian trade-mark laws, there is a very real prospect that the domain name holder could become liable under the laws of a foreign jurisdiction. The facts of such circumstance would be highly relevant-particularly whether the Canadian organization sold goods or services, and had a location in the foreign jurisdiction. As well, such country's willingness to take jurisdiction over a foreign defendant and its characterization of this activity as either a public or private matter would be important considerations.

Relevant Legislation

Foreign jurisdictions' trade-mark, trade name or unfair competition laws (statutory, regulatory or case law)

Self-Aide Practices

(i) Domain name holder should consider incorporating into its Internet site a disclaimer as to the claimed ownership rights to its domain name and related trade-marks and trade names.

(ii) In those foreign jurisdictions where the Canadian organization has a "presence" (e.g. an office, agent etc.) or into which it supplies goods or services, a search and review of trade-mark and trade name rights should be undertaken, with corresponding remedial action depending on the search results.

[Cat. No.: C2-312/1997E ISBN: 0-662-25489-9]

CIVIL LIABILITY: WHO ANSWERS FOR INFORMATION?

Civil Liability: Who Answers for Information?

Introduction

The Internet raises much controversy regarding civil liability. Thus, we must study criteria used to assign liability to the participants in communications occurring on the Internet. In order to account for the diversified manner in which the issue of civil liability is posed on the Internet, two complementary approaches are required. First, we must situate the standards governing the assignment of liability according to the roles adopted by the various participants in electronic communications. Then, in order to go beyond the limitations of an analysis based solely on analogies with roles played in other communications environments, it is necessary to inquire into the factors likely to influence the assignment and degree of responsibility.

The Internet allows many different communications contexts to be established and the variety of these activities makes it impossible to refer to a single traditional means of communication (radio, press, telephone, etc.) to analyze the legal framework of liability[1]. Since the major characteristic of the Internet is its great volatility, depending on the circumstances, the situations which can be encountered there can correspond to various situations which could occur in diverse known communications contexts. Thus, there is a need to consider a plurality of analogies[2].

Metaphors are conceptual tools useful for clarifying the analysis of situations in which we attempt to determine the liability of the various participants in communications taking place in a universe like the Internet. Metaphors[3] can provide clues to the types of relations there are and to the rules which should be applied in various situations[4]. However, we must avoid applying such metaphors mechanically and extending a type of regulation to an electronic environment which is likely to

---

[1] Giorgio Bovenzi, "Liabilities of System Operators on the Internet" (1996) 11 Berkeley Technology Law J., 93 at 130 ff.; David R. Johnson and Kevin A. Marks, "Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) be Our Guide?" (1993) 38 Vill. L. Rev. 487 at 487.

[2] Henry H. Perritt, "Discussion Paper: Metaphors for Understanding Rights and Responsibilities in Network Communities: Print Shops, Barons, Sheriffs and Bureaucracies" Online 15 October 1992, (http:/www.law.vill.edu/chron/articles/metafin.htm).

[3] This way of borrowing existing concepts is not new. Metaphors have long been used in the computer domain. See: David R. Johnson and Kevin A. Marks, *supra*, note 1 at 488.

[4] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 488. See also David Loundy, "Whose Standards? Whose Community?" (1 August 1994) Chicago Daily Law Bulletin, 5, (http:/www.leepfrog.com/E-Law/CDLB/AABBS.html).

present many paradigm cases and is characterized by rapid changes in roles, functions and technical possibilities[5].

Thus, we will study the Internet liability regime, recognizing the varied nature of the Internet environment. We will apply, in consequence, the concepts of liability law, as they have developed to date, while taking into account the various means of communication[6].

---

[5] Richard M. Neustadt, Gregg P. Skall and Michael Hammer, "The Regulation of Electronic Publishing" (1981) 33 Federal Communications Law Journal, 331 at 332.

[6] Eric Schlacter, "Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions" (1993) 16 Hastings Comm/Ent L.J. 87 at 100.

1. Civil Liability Regimes in Canada

Common law includes principles governing civil liability. Since such matters fall into the domain of property and civil rights, they are regulated by provincial legislation. Gerald L. Gall writes that "the Canadian legal system, as a whole, consists of two major components. The private law in nine of the provinces of Canada is governed by the common law system, while in the province of Quebec, private law is governed by a civil law system[7]."

The two systems are very similar in that they establish legal regimes which often lead to equivalent solutions. However, their fundamental approaches have major differences. Civil law systems tend to be based on a set of principles which are most often compiled in an argued set, a code. Individual situations are then decided from the principles which have already been stated in the code. Interpretation can be used to make up for those areas about which the code is silent.

In contrast, the common law approach is to examine the decisions handed down in earlier situations and to induce the principles which should be applied in the situation in question. This explains the great importance placed on previous court decisions[8]. Legislation does play a major role, but it is interpreted from concepts with their sources in principles identified by judges in their successive decisions. This results in a corpus, which is enriched throughout history.

In both the common law provinces and Québec, common law liability regimes are complemented, or sometimes replaced, by certain exception regimes concerning certain enterprises. Federal legislation on certain enterprises falling under Parliamentary jurisdiction can also prescribe civil liability regulations specific to such enterprises.

Common Law

In common law, civil liability is expressed through concepts connected to tort law. As is clear from the definition of the term, "torts" concern justiciable actions with harmful consequences for others. Tort law includes legal regulations specifying the circumstances in which an individual is likely to be found liable for damages caused by a justiciable action[9]. As James and Brown say, "`Torts' are, in the main, those kinds of wrongdoing which have, through the ages, been defined in the cases: which have been evolved by judicial creation, and which continue to be created and

---

[7] Gerald. L. Gall, *The Canadian Legal System*, Third Edition (Toronto: Carswell, 1990) at 49.

[8] *Ibid*. at 28.

[9] Philip S. James and D. J. Latham Brown, *General Principles of the Law of Torts*, Fourth Edition (London: Butterworths, 1978) at 3.

refined?"[10]. Legal recourse based on tort law is essentially oriented toward the goal of compensating for damages suffered.

Civil Law

In civil law, civil liability designates the set of rules which oblige the author of damages to others to provide compensation for the harm[11]. The general principle is stated in Article 1457 of the Civil Code, and rests on the person's fault. It reads as follows:

> Art. 1457. Every person has a duty to abide by the rules of conduct which lie upon him, according to the circumstances, usage or law, so as not to cause injury to another.
>
> Where he is endowed with reason and fails in this duty, he is responsible for any injury he causes to another person and is liable to reparation for the injury, whether it be bodily, moral or material in nature.
>
> He is also liable, in certain cases, to reparation for injury caused to another by the act or fault of another person or by the act of things in his custody.

The evaluation of the fault is the court's responsibility and follows from the facts and circumstances of each case. Tribunals decide on a fault by taking into consideration the behaviour of the person involved and that which a reasonable person would have had under similar circumstances. This search for an objective standard must be performed while first taking into account the context, for example the activity of the actor at the time the injury was caused, and the conditions under which he or she was engaged in such activity[12].

Specific Regimes Established by Legislation

Certain laws deal with specific subjects which may require special rules regarding the liability of certain actors. Thus, Section 31 of the *Telecommunications Act* provides that:

---

[10] *Ibid*. at 3.

[11] Geniève Viney, *Traité de droit civil - Les obligations, La responsabilité, les conditions*, Ed. Jacques Ghestin (Paris: LGDJ, 1982) at 1.

[12] Patrick A. Molinari and Pierre Trudel, "Le droit au respect de l'honneur, de la réputation et de la vie privée: Aspects généraux et applications" in *Formation permanente, Barreau du Québec, Application des chartes des droits et libertés en matière civile* (Cowansville: Yvon Blais, 1988) 197.

> No limitation of a Canadian carrier's liability in respect of a telecommunications service is effective unless it has been authorized or prescribed by the Commission.

The CRTC has approved general provisions on terms of services and certain provisions of these regulations provide for the exclusion of liability. Thus Article 16.2 of the terms of services provides that telecommunications carriers are not liable for:

> - defamation arising from material transmitted over the carrier's facilities;
>
> - infringement of patents arising from the combining of carrier facilities and customer-owned facilities;
>
> - copyright infringement arising from the transmission of material over carrier facilities;
>
> - in the case of directory advertisements or customer listings, copyright or trademark infringement, passing off and acts of unfair competition, provided the advertisements or the information contained in the listings was received in good faith in the ordinary course of business.[13]

Michael Ryan writes that:

> It is open to question whether the [...] CRTC has the jurisdiction to regulate liability in respect of such matters as defamation, patent and copyright infringement, passing off and acts of unfair competition in the circumstances described in art. 16.2.[14]

In effect, in *Clark* v. *Canadian National Railways*[15], the Supreme Court decided that the imposition of limits on recourse resulting from liability following from such events fell into the domain of Property and Civil Rights and was thus under provincial jurisdiction. Ryan also wonders if Parliament can limit liability resulting from copyright or trademark infringement as it does in Article 16.2[16].

---

[13] Michael H. Ryan, *Canadian Telecommunications Law and Regulation* (Toronto: Thompson Canada, 1993) at 4-19.

[14] *Ibid.*

[15] *Clark* v. *Canadian National Railways* [1988] 2 S.C.R., 680.

[16] Michael H. Ryan, *supra*, note 13 at 4-20.

Moreover, the terms of Section 31 of the *Telecommunications Act* can appear insufficiently explicit to allow one to conclude with certainty that, in them, Parliament intended to target subjects such as civil liability for defamation and other similar issues.

2.Overview of Internet Situations Generating Civil Liability

The more the Internet becomes the site of multiple interactions, the more it becomes a potential theatre of conflict between the participants in the various communications situations it makes possible. Attacks on reputation and on other interests are among the situations for which it is necessary to situate the responsibilities of the participants in Internet communications.

In this respect, Michael McCormack notes that:

> Unfettered free speech on the Internet is now a thing of the past. [...] Already more than 100 civil actions have been raised for libel in the US after unflattering comments were made in forums, discussion groups, and even on E-mail.[17]

Yet the Internet is a multifaceted universe: it is not always easy to evaluate the size of the problems likely to engender liability. As Braithwaite and Carolina point out, the sizes made familiar to us by traditional media contexts are no longer necessarily the same on the Internet:

> The inevitable effect of the multimedia revolution is a deluge of information, so users will have to filter inflows, while authors will strive to target their output more specifically. A libel juror might reasonably ask how seriously a plaintiff's reputation is harmed by relatively narrowcast bulletin board defamation, in comparison with the widespread damage caused by a broadcast of printed libel. Given the specialised nature of bulletin boards, such scepticism would be misplaced. In the academic community, for example, bulletin boards are often the chosen method of correspondence in certain fields of study. Scurrilous bulletin board messages, even if not widely disseminated by conventional mass media standards, may be nicely targeted to achieve maximum damage to professional or business reputation.[18]

We shall thus examine the principal situations which generate civil liability on the Internet, and how the regulations applicable to such situations are formulated at present.

---

[17] Michael McCormack, "Tell it to the Judge," .net, issue 9, August 1995 at 60.

[18] Nick Braithwaite and Robert Carolina, "Multimedia Defamation" International Media Law, March 1994 at 19.

Defamation and Harm to Reputation

Potts and Harris remind us that "The law of defamation seeks to balance two opposing interests: on the one hand there is freedom of speech; on the other, the importance of reputation. In a cybersociety or wired world, both of these interests are increasingly important."[19] Defamation law, due to its ancient origins, provides many concepts regarding liability resulting from the circulation of information in a network environment. These principles are, in effect, relevant to most situations in which an individual could complain of harm done to interests linked to himself or herself.

The Supreme Court of Canada asserts the importance of protecting the reputation of persons and recognizes the links between such protection and more recent notions such as that of privacy. In *Hill v. Church of Scientology* case, Cory J. wrote that:

> Although it is not specifically mentioned in the *Charter*, the good reputation of the individual represents and reflects the innate dignity of the individual, a concept which underlies all of the *Charter* rights. It follows that the protection of the good reputation of an individual is of fundamental importance to our democratic society.
>
> [§]121 Further, reputation is intimately related to the right to privacy which has been accorded constitutional protection. As La Forest J. wrote in *R.* v. *Dyment*, [1988] 2 S.C.R. 417, at 427, privacy, including informational privacy, is "[g]rounded in a man's physical and moral autonomy" and "is essential for the well-being of the individual." The publication of defamatory comments constitutes an invasion of the individual's personal privacy and is an affront to that person's dignity. The protection of a person's reputation is indeed worthy of protection in our democratic society and must be carefully balanced against the equally important right of freedom of expression.[20]

Protection of the reputation of persons is taken care of by defamation regimes in each of the provinces. The liability assumed for the publication of defamatory statements extends to all those who participate in any way in the dissemination of defamation. Thus, the editor, the section head, the owner of the newspaper and even the person who participates in its distribution can be held liable. In fact, any individual who knows or should know of the defamatory nature of the statements, or has a degree of control over the dissemination of the statements, is potentially

---

[19] David Potts and Sally Harris, "Defamation on the Internet", Paper prepared for a conference entitled "Legal Issues on the Internet", Toronto, 14 May 1996 at 9.

[20] *Hill* v. *Church of Scientology* [1995] 2 S.C.R. 1130 at 1179.

liable.[21] This is why the transposition of many of these principles to the universe of the Internet raises numerous questions.

We will summarize the Common law and civil law principles.

In Common Law

In *Hill* v. *Church of Scientology*, Cory J. thus reviews the origins of defamation law:

> The character of the law relating to libel and slander in the 20th century is essentially the product of its historical development up to the 17th century, subject to a few refinements such as the introduction and recognition of the defences of privilege and fair comment. From the foregoing we can see that a central theme through the ages has been that the reputation of the individual is of fundamental importance. As Professor R. E. Brown writes in *The Law of Defamation in Canada* (2nd ed. 1994), at p. 1-4:
>
> "(N)o system of civil law can fail to take some account of the right to have one's reputation remain untarnished by defamation." Some form of legal or social constraints on defamatory publications "are to be found in all stages of civilization, however imperfect, remote, and proximate to barbarism." [footnotes omitted]
>
> [§] 117 Though the law of defamation no longer serves as a bulwark against the duel and blood feud, the protection of reputation remains of vital importance. As David Lepofsky suggests in "Making Sense of the Libel Chill Debate: Do Libel Laws 'Chill' the Exercise of Freedom of Expression?" (1994), 4 N.J.C.L. 169, at p. 197, reputation is the "fundamental foundation on which people are able to interact with each other in social environments." At the same time, it serves the equally or perhaps more fundamentally important purpose of fostering our self-image and sense of self-worth. This sentiment was eloquently expressed by Stewart J. in *Rosenblatt* v. *Baer*, 383 U.S. (1966), who stated at p. 92:
>
> The right of a man to the protection of his own reputation from unjustified invasion and wrongful hurt reflects no more than our basic concept of the essential dignity and worth of every human being - a concept at the root of any decent system of ordered liberty.[22]

A defamation action is made up of three elements. The plaintiff must demonstrate that the defamatory charge was published. What is meant by publication is that the offending statements

---

[21] Michael G. Crawford, *The Journalist's Legal Guide*, Second Edition (Agincourt, Ontario: Carswell, 1990) at 16.

[22] *Hill* v. *Church of Scientology* [1995] 2 S.C.R. 1130 at 1177-1178.

were made known by some one other than their author. Second, the plaintiff must establish that the defamation indeed refers to himself or herself. Third, the plaintiff must establish that the charge is defamatory, in other words that it is false and that it discredits him or her.

Once proof of publication has been made, the plaintiff has the advantage of a number of presumptions. In effect, it is presumed, subject to evidence to the contrary, that the charge is false, that it was published with malice and that the plaintiff suffered damages.

Thus, in Australia, the Supreme Court considered in *Rindos* v. *Hardwick*[23] that the statements disseminated in a discussion list could be defamatory and lead to a liability action. The court did not judge it appropriate to treat the Internet context as different from already known means of communication, and recognized the author's responsibility for the defamatory statements transmitted in a discussion group[24]. The issue of the liability of the other participants was, however, not discussed.

In defence, the defendant can have the presumptions existing in the plaintiff's favour ruled out by establishing that the statements were true or constituted a fair comment. The defendant has the right to comment on true facts if he or she is not motivated by malice, or if he or she invokes privilege. The notion of privilege refers to situations in which the law or the tribunals consider that an individual must be free to publish certain statements without having to assume liability for their defamatory nature. Privileges may be absolute, such as declarations made in a parliament by parliamentarians, or qualified, such as when publication is judged unnecessary or tainted with malice. Finally, common law recognizes the "innocent dissemination" defence, which proves to be especially important in the context of the Internet.

In Canada, the rules regarding innocent dissemination are based on relatively old jurisprudence[25] according to which it is admissible for a person to invoke such a defence under the following three conditions, as stated by Brown:

> He was innocent of any knowledge of the libel contained in the work disseminated by him;

---

[23] In the Supreme Court of Western Australia between David Rindos and Gilbert John Hardwick, Heard: 25 March 1994. Delivered: 31 March 1994. No. 1994 of 1993 (Unreported judgement 940164) http://www.law.auckland.ac.nz/cases/Rindos.html.

[24] Gareth Sansom, *Illegal and Offensive Content on the Information Highway* (Ottawa: Industry Canada, 1995) (http://www.ic.gc.ca/info-highway/offensive/offens_e.rtf). See also Henry H. Perritt, *supra*, note 2.

[25] *Newton* v. *Vancouver* (1932) 46 B.C.R. 67, 75.

> There was nothing in the work or in the circumstances under which it came to him or was disseminated by him that ought to have lead him to suppose that it contained a libel;
>
> That when the work was disseminated by him it was not by any negligence on his part that he did not know that it contained the libel, then although the dissemination of the work by him was *prima facie* a publication of it, he may nevertheless, on proof of the before mentioned facts, be held not to have published it.[26]

David Potts and Sally Harris point out that one consequence of the rules concerning innocent dissemination is that online information services and Internet access providers are placed in a delicate position.

> By exercising responsibility and attempting to regulate the nature of the content, the online service provider may then become a publisher and can be sued for libel. On the other hand, if they do absolutely nothing, they could be sued for negligence for failing to maintain security, or for negligent misstatement.[27]

Thus, given the present state of defamation law, we cannot exclude the possibility that an intermediary could be called to answer for defamation suffered by a person due to information circulating in a network over which the intermediary exercised some control.

The lack of precedents and the relatively strict nature of defamation rules lead us to think that there are real possibilities that many actors in Internet communications could be called upon to answer for defamatory statements. It could be considered that at the present state of development of the law, computer network owners and operators could be held responsible for defamatory materials, whether they write them themselves or publish them after having received them from third parties. Thus, a company could be obliged to assume liability for statements found on its electronic sites.

In Civil Law

The situation appears more or less the same in civil law. Under Québec law, harm to reputation is governed by the general principles of civil liability[28]. Thus, the notion of civil fault is what

---

[26] Raymond E. Brown, *The Law of Defamation in Canada*, Second Edition at 7.12(6).

[27] David Potts and Sally Harris, *supra*, note 19 at 20.

[28] *Art. 1457. Every person has a duty to abide by the rules of conduct which lie upon him, according to the circumstances, usage or law, so as not to cause injury to another. Where he is endowed with reason and fails in this duty, he is responsible for any injury he causes to another person and is liable to reparation for the injury, whether it be bodily, moral or material in nature...*

determines the extent of the right to respect for the reputation of an individual with respect to third parties. Article 3 of the Québec *Civil Code* provides that:

> Art. 3. Every person is the holder of personality rights, such as the right to life, the right to the inviolability and integrity of his person, and the right to the respect of his name, reputation and privacy.
>
> These rights are inalienable.

This provision restates that of Section 4 of the *Charter of Human Rights and Freedoms*, which provides that: "Every person has a right to the safeguard of his dignity, honour and reputation."[29]

Through analyzing the circumstances resulting in recourse for actionable harm to reputation, it is possible to identify the extent of the notion of protection of reputation[30]. Generally, doctrine and jurisprudence have established that harm to reputation is actionable in circumstances in which it is unjustified and, more specifically, in cases of abuse of confidence, harassment and defamation.

Harm to reputation can be intentional or unintentional. According to Baudouin, under Québec civil law, justiciable harm to reputation can result from two types of behaviour:

> [TRANSLATION] The first is that of a defendant who knowingly, in bad faith and intending to injure, harmed the victim's reputation and tried to ridicule or humiliate the victim, or to expose him or her to public hatred or contempt or to the hatred or contempt of a group. The second results from conduct in which, although there is no will to injure, the defendant nevertheless harmed the victim's reputation through recklessness, negligence, impertinence or carelessness.[31]

---

[29] *Charter of Human Rights and Freedoms*, R.S.Q. c. C-12.

[30] [TRANSLATION] "*Traditionally, the law punishes intentional or unintentional harm to the reputation of another. It is recognized at the outset that any expression relating to an individual's person or acts could ultimately affect his reputation. This undoubtedly explains why the very concept of the right to safeguard one's reputation has the potential for being confused with that of harm to one's reputation, or defamation. This right therefore does not grant a general power to prevent the dissemination of information we find embarrassing; rather, it concerns disseminations that would not be carried out by a prudent and diligent person in similar circumstances."* P. A. Molinari and P. Trudel, *supra*, note 12 at 202.

[31] J.-L. Baudouin, *La Responsabilité Civile*, Fourth Edition (Yvon Blais, 1994) No. 417 at 236-237.

> The right to freedom of expression cannot therefore be used solely to harm another person.[32]

The courts determine fault using three criteria: 1) the difference between the actor's behaviour and that which a reasonable, diligent person would have had in similar circumstances; 2) the activity of the actor, and the conditions in which he or she undertook such activity, at the time the prejudice was caused; and 3) the public interest.

The difference between the behaviour of the actor and that which a reasonably prudent and diligent person would have had is determined through an attempt to establish standards. The standard of a prudent, diligent person is an objective concept[33]. In the framework of reflection on this concept, the truth[34] or the falsehood[35] of the statements made can be taken into consideration. For example, in certain situations when the falsehood of the allegations is established, the court could infer that the defendant had not taken all the precautions that a reasonable person would have taken to avoid publishing falsehoods[36]. Courts also take into account the status of the person defamed: in other words, whether the person is public or private. Thus, they are more tolerant with respect to statements disseminated regarding a public person. In this respect,

---

[32] *Ibid*. at 236.

[33] P. A. Molinari and P. Trudel, *supra*, note 12 at 204.

[34] [TRANSLATION] *"It is well established in our law of civil liability that good faith is not a factor that can exonerate a person who commits a wrongful act . . . It is . . . only where the facts alleged in the message at issue in the action are true that the defendant can argue that any conclusions he drew from those facts were drawn in good faith. Good faith can then be taken into consideration even if what was inferred from the facts was actually wrong. As a result, mere honest belief in the accuracy of the information or of the inferences is not enough."* P. A. Molinari and P. Trudel, *supra*, note 12 at 206-207.

[35] Note that the falsehood of the statements is not an element of defamation.

[36] P. A. Molinari and P. Trudel, *supra*, note 12 at 204. See also, *Bombardier* v. *Bouchard* J-E 96-731 (C.A.): [TRANSLATION] *"The freedom to express an opinion on a question of public interest is protected, but only where the defamatory opinion is an honest expression of the point of view of the person expressing it. It is up to the defamer to satisfy the court that his or her allegations are authentic. In calling the respondent a pedophile, the appellant knew she was not telling the truth or was at the very least being reckless. In so doing, she disregarded her duty and must bear a reasonable level of responsibility for having harmed the respondent's honour, dignity and personal and professional reputation."*

Baudouin writes that [TRANSLATION] "public persons, like political personalities, can expect to be attacked more often than others, and the tolerance for abuse must be higher in their case"[37].

According to Vallières, the public interest is a "just motive" for revealing unflattering information regarding an individual. She argues that since it serves the public's right to information, public interest makes defamation legitimate[38].

The context in which defamation occurs is thus a major variable in the evaluation of behaviour[39]. The courts take into account, in particular, the activities of the individual at the time the defamatory statements were transmitted[40], the type of information disseminated[41], the context[42] in which the statements were disseminated[43]. In a context characterized by a multitude of actors,

---

[37] J.-L. Baudouin, *supra*, note 32 at 238. Molinari and Trudel, referring to Vallières and Sauvageau, note however that [TRANSLATION] *"criticism of public persons does not mean that it is justifiable to shower them with personal insults or make up falsehoods. Similarly, an error of judgment committed by a person in performing his or her duties is no justification for saying he or she is dishonest."* in P. A. Molinari and P. Trudel, *supra*, note 12 at 207.

[38] N. Vallières, *La presse et la diffamation* (Montréal: Wilson et Lafleur, 1985) at 90. See also P. A. Molinari and P. Trudel, *supra*, note 12 at 220-221: [TRANSLATION] *"Thus, the right to respect for one's reputation and privacy will be limited by the public's interest in knowing about certain aspects of a person's character in order to decide, inter alia, whether he or she continues to deserve the public's trust."*

[39] [TRANSLATION] *"Fault is not based solely on an abstraction. The classic example of the prudent individual is not universal, the same in every sphere of activity. A subjective element must be added to the abstract model of the "reasonable person". In assessing fault, the person's occupation and the circumstances of engaging in it must be taken into account."* in N. Vallières, *supra*, note 39 at 58.

[40] P. A. Molinari and P. Trudel, *supra*, note 12 at 204.

[41] P. A. Molinari and P. Trudel, *supra*, note 12 at 205. These authors refer in particular to the typology proposed by Chevalier J. in *Fabien* v. *Dimanche Matin*, which set out three categories of messages: the relation of material facts, the reminder of statements made, and the commentary.

[42] [TRANSLATION] *"The courts must also consider the context of the abuse or defamation. In certain especially heated exchanges, they sometimes accept a "set-off" for abuse, that is, the defence of provocation, provided first that the exchange was simultaneous and second that the abuse in response to the provocation was uttered immediately."* in J.-L. Baudouin, *supra*, note 32 at 238.

[43] P. A. Molinari and P. Trudel, *supra*, note 12 at 204-207.

when many people are united in a common undertaking of public dissemination, the rule of single publication can be applied.

Thus, each person who has participated in the dissemination assumes part of the liability since each was involved in a shared process going from the publication to the sale of the newspaper[44]. Under civil law, the coauthors of a harmful act are held to have joint responsibility, even if the responsibility of one of the authors is personal and direct and that of the other subsidiary. However there must be a clear link between the coauthors and the prejudice suffered[45]. In a context such as that of Internet transmission, characterized by the presence of many different actors, when a number of people are united in a shared undertaking of public dissemination, it is appropriate to apply the rule of single publication.

In consequence, given the way in which rules concerning liability are applied with respect to defamation, the various intermediaries who make possible the transmission of information on the Internet could be assigned a share of the liability following from statements causing injury to the reputation of a person. Application of the principle of joint responsibility gives the victim of actionable harm the right to claim the totality of damages from one of the intermediaries, even if such an intermediary could be assigned only a minute share of the liability.

---

[44] Nicole Vallières, *supra*, note 39 at 71.

[45] André Nadeau and Richard Nadeau, *Traité pratique de la responsabilité civile délictuelle* (Montréal: Wilson & Lafleur, 1971) at 572.

Invasion of Privacy

There appears to be a consensus on the need to protect privacy, honour and reputation in electronic environments. Opinions may differ, however, on the degree of protection which should be offered and the way in which it should be applied. In both of Canada's legal systems, there are provisions imposing liability for invasion of privacy.

In Common Law

Under Canadian common law, unlike that which is accepted and applied in the United States, there is no recognition as such of the right to privacy[46]. Burns writes in this respect that "At a superficial level, the common law of privacy is simple to summarize: there is no protection for personal privacy *per se*, at least outside of the United States."[47] Fleming explains this situation as follows:

> The right of privacy has not so far, at least under that name, received explicit recognition by British courts. For one thing, the traditional technique in tort law has been to formulate liability in terms of reprehensible conduct rather than of specified interests entitled to protection against harmful invasion. For another, our courts have been content to grope forward, cautiously along the grooves of established legal concepts, like nuisance and libel, rather than make a bold commitment to an entirely new head of liability.[48]

While in the Commonwealth there does not seem to be a general right to privacy, some torts cover certain aspects of such a right. In this vein, Burns identifies the torts of trespass to land, trespass to chattels, trespass to the person, nuisance, defamation, injurious falsehood, wilful infliction of nervous suffering, passing off, and breach of confidence.

---

[46] See, in general: Karim Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'informations* (Montréal: Éditions Thémis, 1992) at 13 ff. See also: Philipp H. Osborne, "The Privacy Acts of British Columbia, Manitoba and Saskatchewan" in Dale Gibson, *Aspects of Privacy Law, Essays in Honour of John M. Sharp* (Toronto: Butterworths, 1980) at 73-108.

[47] Peter Burns, "Privacy and the Common Law: A Tangled Skein Unravelling?" in Dale Gibson, *supra*, note 47 at 21-40. See also Peter Burns, "The Law of Privacy: The Canadian Experience" [1976] 54 Can. Bar. Rev., 1, at 12. Regarding Australian law, Skala makes the same remark: It can be stated with some confidence that Anglo-Australian law does not recognise the existence of a legal right to privacy." S. M. Skala, "Is There a Legal Right to Privacy?" [1977-78] Queensland L. J., 127 at 133.

[48] Fleming, *The Law of Torts*, 5th Ed., 1977 at 590-591; cited in Peter Burns, "Privacy and the Common Law: A Tangled Skein Unravelling?" in Dale Gibson, *supra*, note 47 at 22.

In the United States, the notion of "privacy" appeared quite recently in the vocabulary of jurists. Warren and Brandeis[49] are credited with the idea that privacy should appear among the rights protected by the Constitution. The approach they developed was, in the end, to become so prevalent that the Supreme Court, after several decisions in which it denied the existence of privacy as a constitutional right, finally endorsed it[50].

Warren and Brandeis's point of view was not accepted spontaneously by the tribunals. The first major judicial decision to be made on arguments in favour of the recognition of a right to privacy was *Roberson* v. *Rochester Folding Box Co.*[51]. A company was sued for having used the plaintiff's picture on advertising posters. By a majority of four to three, the court rejected the action, but not without abundant discussion of the point of view developed in the Warren and Brandeis article. The decision of the majority judges demonstrates scepticism of the existence of the right to privacy in common law. The judges were worried about the scope such a right could take if it were recognized in such a case. They even added that the behaviour of which the plaintiff complained could please others who could ask for nothing better than to see their own image reproduced on a large scale.

This decision sparked a movement in opinion toward legislative recognition of the right to privacy. The New York State legislature adopted an act providing for a prohibition on the commercial use of the name, picture or portrait of a living person without first obtaining their written authorization[52]. This act inspired many developments in jurisprudence[53] and served as a model for a number of states wanting to adopt a regime of privacy protection.

In other states, the law evolved rather toward the gradual recognition of a right to privacy based on common law precedents. In the 1920's and 1930's, the courts began to receive actions undertaken because of invasions of privacy resulting from the publication of information of which the truth was not questioned.

---

[49] E. A. Warren and L. Brandeis, "The Right to Privacy" (1890) Harv. L. R. 193.

[50] *Griswold* v. *Connecticut* 381 U.S. 479 at 485 (1965).

[51] 171 N/Y., 538, 64 N.E., 442 (1902).

[52] T. Barton Carter, Marc A. Franklin and Jay B. Wright, *The First Amendment and the Fourth Estate - The Law of Mass Media*, Fourth Edition (Westbury: The Foundation Press, 1988) at 157-158.

[53] Harold L. Nelson, Dwight L. Teeter Jr. and Don R. Le Duc, *Law of Mass Communications - Freedom and Control of Print and Broadcast Media*, Sixth Edition (Westbury: The Foundation Press, 1989) at 247.

As of the end of the 1930's, the courts began to show themselves to be more attentive to the still emerging tendency of the Supreme Court to extend media protection by basing itself on the First Amendment. Thus, with respect to private facts embarrassing to the individuals targeted, the courts developed a defence based on the value of the information as news: its "newsworthiness". This notion was to be used as a defence regarding the publication of virtually any information considered by the editors to be likely to interest readers. This defence was so effective that in the 1960's many doubted that any recourse for invasion of privacy could survive.

However, during the 1960's and 1970's, the notion of privacy moved back to the top of the public agenda due to concerns raised by the development of computer data banks and to increasingly outrageous invasions by certain media. The notion of privacy was thus taken up again in Supreme Court decisions, which used it to determine the constitutional validity of legislation on marriage[54], abortion[55], birth control[56], and obscenity[57]. The principle emphasized was that government authorities need not interfere in personal choices. The Supreme Court's use of the notion of "privacy" to analyze the validity of various measures was to widen the field of the notion.

In Canada, in *Hunter*[58] and especially in *Dyment*[59], the Supreme Court recognized that the right to privacy was protected to a certain degree by the constitution, at least in situations in which there was a legitimate expectation of privacy.

---

[54] *Loving* v. *Virginia*, 388 U.S., 1 (1967).

[55] *Roe* v. *Wade*, 410 U.S., 113 (1973).

[56] *Griswold* v. *Connecticut*, 381 U.S., 484 (1965). Regarding this major decision, see "25th Anniversary of *Griswold* v. *Connecticut* and the Right to Privacy" (1989) 16 Ohio Northern University L.R., 359; *Eisenstadt* v. *Baird*, 405 U.S. 438 (1972); *Carey* v. *Population Services International*, 431 U.S., 678 (1977).

[57] *Stanley* v. *Georgia*, 394 U.S. 557.

[58] *Hunter* v. *Southam*, [1982] 2 S.C.R. 145.

[59] *R.* v. *Dyment*, [1988] 2 S.C.R. 417. The *Dyment* decision even recognized an information aspect of privacy. Regarding this, see Karim Benykehlef, *supra*, note 47 at 29.

The determination of the outlines of the notion of "privacy" and of what it protects continues to raise many questions[60]. Four types of behaviours have been recognized by the courts as attacks on privacy: these forms of behaviour were classified by Prosser and then recognized in the *Restatement of Torts*. They are intrusion, publicity of private facts, false light and appropriation. The making public of private facts is clearly the heart of the notion of privacy. The three other forms of behaviour are linked to privacy in many ways, but also belong to other universes.

Legislation in Saskatchewan, Manitoba, Newfoundland and British Columbia

In Saskatchewan, Manitoba, Newfoundland and British Columbia, invasion of privacy is a tort for which an action can be instituted, without proof of damage, against any person who knowingly[61] and unrightfully violates the privacy of another person.[62]

Notably, the following activities constitute *prima facie* evidence of invasion of the privacy of a person:

1. Audio or visual surveillance of that person, whether or not it is accomplished through *trespass*, including the action of eavesdropping on, watching, spying on, or following that person.[63]

2. Unless such actions are accomplished by a party lawfully authorized to do so, the listening to or recording of a conversation in which that person participates, or the

---

[60] Jed Rubenfeld, "The Right of Privacy" (1989) 102 Harvard L. R., 737 at 751.

[61] In Manitoba, this fact is classed among defences in Section 5 (1) (b) of *The Privacy Act* R.S.M. c. P-125: "In an action for violation of privacy of a person, it is a defence for the defendant to show that the defendant, having acted reasonably in that regard, neither knew or should reasonably have known that the act, conduct or publication constituting the violation would have violated the privacy of any person..."

[62] *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 2. *The Privacy Act*, R.S.M. c. P-125 s. 2 (1)-2 (2). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 3 (1). *Privacy Act*, R.S.B.C. c. 336 s. 1 (1).

[63] *Privacy Act*, R.S.B.C. c. 336 s. 1 (4). *An Act respecting the protection of Privacy*, R.S.S. c. P-24 s. 3 (1) (a). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 4 (a). Note that the latter also mentions the action of harassment. *The Privacy Act*, R.S.M. c. P-125 s. 3 (a). Note that the latter specifies that as well as activities which could harm a person himself or herself, there are activities targeting his or her house or any other place of residence and his or her motor vehicle.

listening to or recording of messages travelling to or coming from that person through telecommunications means.[64]

Contrary to the acts in Newfoundland and Saskatchewan, the act in Manitoba does not provide explicit protection for messages travelling over *telecommunications* media. Indeed, Section 3 (b) specifies only messages sent over the telephone.[65] The much more succinct wording of the British Columbia act seems to provide protection for all private communications of a person, no matter what the means of communication (or media on which the information is carried). Thus, Section 1 (4) of the *Privacy Act*[66] provides simply that invasion of privacy can occur through surveillance or eavesdropping.

3. The use of that person's letters, personal diaries or other personal documents.[67]

Note that the British Columbia legislation is the only one which does not explicitly mention this activity.

4. The use of the name, likeness[68] or voice of that person for the ends of any advertising or sales promotion of any property or service, or other commercial activity, if, in the course of such activity the person is identified or identifiable and the user intended to exploit the person's name, likeness or voice.[69]

---

[64] *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 4 (b). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 3 (1) (b). *The Privacy Act*, R.S.M. c. P-125 s. 3 (b).

[65] *The Privacy Act*, R.S.M. c. P-125 s. 3 (b).

[66] *Privacy Act*, R.S.B.C. c. 336.

[67] *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 4 (d). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 3 (1) (d). *The Privacy Act*, R.S.M. c. P-125 s. 3 (d).

[68] Note that unlike in the other provinces which use the expression "likeness" in such legislation, in British Columbia, in Section 3 (1) of the *Privacy Act* R.S.B.C. c. 336, the expression "portrait" is used instead. The expression "portrait" seems to us to be more precise.

[69] *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 3 (1) (c). *The Privacy Act*, R.S.M. c. P-125 s. 3 (c). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 4 (c). *Privacy Act*, R.S.B.C. c. 336 s. 3 (1).

The British Columbia act is more precise regarding the extent of the right to one's name. Thus, in Section 3 (2) of the *Privacy Act*[70], it states that there is no invasion of privacy when a name identical to the plaintiff's name, or so similar to the plaintiff's name that it could be mistaken for it, is used unless the court is satisfied 1) that it was used with the specific intention to refer to the plaintiff or to exploit his or her name or reputation (s. 3 (2) (a)), or 2) that it was used in the course of commercial activities in such a way that it could be associated in the mind of the public, implicitly or explicitly, with the plaintiff's person such that the plaintiff could be distinguished from another person with a similar or identical name (s. 3 (2) (b)).

The same applies for the extent of the right to one's likeness. Thus, Section 3 (3)[71] states that there is no invasion of privacy when use is made of the plaintiff's portrait in a photograph of a group of persons unless 1) he or she is identified by name or description, or there is special emphasis on his or her presence, or 2) he or she is identifiable and the user had the specific intention of employing the plaintiff's likeness in order to exploit his or her name or reputation. In Section 3 (4)[72], the conditions are set on the use of the name and likeness of a person by the media.

Finally, contrary to the three other acts, the British Columbia act does not make explicit mention that a person's right to privacy includes the protection of his or her voice.

Extent of Protection of Privacy

The nature and degree of protection of privacy to which a person has a right is that which is reasonable under the circumstances, taking into account the interests of third parties.[73] In order to evaluate whether an act, conduct or publication constitutes an invasion of the privacy of a person, the legislation states that the courts must take into account the elements related to its nature, incidence or occasion[74].

---

[70] *Privacy Act*, R.S.B.C. c. 336.

[71] *Privacy Act*, R.S.B.C. c. 336.

[72] *Privacy Act*, R.S.B.C. c. 336.

[73] *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 3 (2). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 6 (1). *Privacy Act*, R.S.B.C. c. 336 s. 1 (2).

[74] *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 3 (2). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 6 (2) (a). *Privacy Act*, R.S.B.C. c. 336 s. 1 (3). *The Privacy Act*, R.S.M. c. P-125 s. 4 (2) (a).

Evaluation of the Degree of Invasion of Privacy

In order to evaluate the degree of the invasion of privacy, the legislation provides that the courts must take into account, in particular, the relation, whether it is familial or otherwise, which may exist between the parties to the action.[75] Except in British Columbia, the legislation provides that the courts must also be attentive to the effect of the violation on the health and well-being, and the social, financial, or business position of the victim and his or her family.[76] Except in Newfoundland and British Columbia, the law provides that the courts must also take into account the conduct of the parties, both before and after the events in question, including an excuse or settlement offer made by the defendant.[77]

Defences

The explicit or implicit consent of the person targeted by the invasion of privacy, or of any person legally authorized to consent in his or her place, allows the author of the action in question to be exonerated.[78] Likewise, an act, conduct or publication which occurs under the following circumstances are not invasions of privacy:

1. when the act, conduct or publication was incidental to the protection of a lawful right of defence of person or property;[79]

---

[75] *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 6 (2) (c); *The Privacy Act*, R.S.M. c. P-125 s. 4 (2) (c); *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 3 (2); *Privacy Act*, R.S.B.C. c. 336 s. 1 (3).

[76] *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 6 (2); *The Privacy Act* R.S.M. c. P-125 s. 4 (2) (b). Note that in Section 1 of the Manitoba act, "family" is defined as follows: "the husband, wife, child, step-child, parent, step-parent, brother, sister, half-brother, half-sister, step-brother, step-sister, of a person." In Section 6 (2) (b) of the Saskatchewan act, "family" and "relatives" are mentioned, but not defined. Furthermore, in Section 4 (2) (d) of the Manitoba act, it is stipulated that the court shall take into consideration "any distress, annoyance or embarrassment suffered by that person or his family arising from the violation of privacy".

[77] *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 6 (2) (d). *The Privacy Act*, R.S.M. C. p-125 S. 4 (2) (e).

[78] *An Act respecting the Protection of privacy*, R.S.S. c. P-24 s. 3 (1) and s. 4 (1). *The Privacy Act* R.S.M. c. P-125 s. 5 (1). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 4. *Privacy Act* R.S.B.C. c. 336 s. 2 (1) (a).

[79] *Privacy Act* R.S.B.C. c. 336 s. 2 (1) (b). *An Act Respecting the Protection of Personal Privacy* R.S.N. c. P-22 s. 5 (1) (b). *An Act respecting the Protection of Privacy* R.S.S. c. P-24 s. 4 (1) (b). *The Privacy Act* R.S.M. c. P-125 s.

2. when the act, conduct or publication was authorized or required by a law in force in the province or by a court or by any process of a court;[80]

3. when the act, conduct or publication was performed by an officer of the peace in the course of his or her duties[81] or by a public officer engaged in an investigation in the course of his or her duty[82], under the condition that the act, conduct or publication was neither disproportionate to the gravity of the matter subject to investigation, nor committed in the course of a trespass.[83]

4. when the act, conduct or publication was performed by a person engaged in a news gathering for a newspaper containing public news[84] or

---

5 (c). In the last section, there are two more elements than in the other Canadian acts: 1) the act, conduct or publication must be not only "incidental" to, but also "necessary" and "reasonable" to the exercise of a lawful right of defence of person or property; 2) the act, conduct or publication in issue may also be intended to protect another interest of the defendant, or of a person who instructed the defendant to so act, or for the benefit of whom the defendant acted.

[80] *Privacy Act* R.S.B.C. c. 336 s. 2 (1) (c). *An Act respecting the Protection of Privacy* R.S.S. c. P-24 s. 4 (1) (c). *The Privacy Act*, R.S.M. c. P-125 s. 5 (d). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 4 (c). In s. 1 of *The Privacy Act* of Manitoba, R.S.M. c. P-125, "court" is defined as follows: "the Court of Queen's bench except in section 5 where it means any court and includes a person authorized by law to take evidence under oath for the purposes for which he is authorized to take evidence." Section 5 (3) (a) of *An Act Respecting the Protection of Personal Privacy* R.S.N. c. P-22 is along the same lines.

[81] *Privacy Act* R.S.B.C. c. 336 s. 2 (1) (d) (i). *An Act respecting the Protection of Privacy* R.S.S. c. P-24 s. 4 (1) (d) (i). *The Privacy Act*, R.S.M. c. P-125 s. 5 (e) (i). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 5 (d) (i).

[82] *Privacy Act* R.S.B.C. c. 336 s. 2 (1) (d) (ii). *An Act respecting the Protection of Privacy* R.S.S. c. P-24 s. 4 (1) (d) (ii). *The Privacy Act*, R.S.M. c. P-125 s. 5 (e) (ii). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 5 (d) (ii).

[83] *Privacy Act* R.S.B.C. c. 336 s. 2 (1) (a). *An Act respecting the Protection of Privacy* R.S.S. c. P-24 s. 4 (1) (d). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 5 (d). Note that in Manitoba, the act, conduct or publication must also have been reasonably necessary in the public interest. See s. 5 (e) of *The Privacy Act* R.S.M. c. P-125.

[84] *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 4 (1) (e) (i).

for a broadcaster[85] under the condition that it was reasonable under the circumstances and necessary or incidental to the usual activities in a press conference.[86] Note that the law in British Columbia does not mention this specific defence, but it does provide a framework for the use of a person's name or portrait by the media in Section 3 (4).[87]

A publication is not an invasion of privacy under circumstances in which there are reasonable justifications for believing that it contains information which is in the public interest[88], that it is fair comment on a matter of public interest[89] or that it is privileged, in accordance with the rules relating to defamation.[90]

---

[85] *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 4 (1) (e) (ii).

[86] *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 4 (1) (2). The Manitoba act does not mention this requirement.

[87] *Privacy Act*, R.S.B.C. c. 336.

[88] *Privacy Act*, R.S.B.C. c. 336 s. 2 (2) (a). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 4 (2) (a). *The Privacy Act*, R.S.M. c. P-125 s. 5 (f) (i). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 5 (2) (a).

[89] *Privacy Act*, R.S.B.C. c. 336 s. 2 (2) (a). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 4 (2) (a). *The Privacy Act*, R.S.M. c. P-125 s. 5 (f) (iii). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 5 (2) (a).

[90] *Privacy Act*, R.S.B.C. c. 336 s. 2 (2) (b). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 4 (2) (b). *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 5 (2) (b). *The Privacy Act*, R.S.M. c. P-125 s. 5 (f) (ii). In Section 1 of *The Privacy Act*, R.S.M. c. P-125, "defamation" is defined as: "libel or slander".

Compensation and Other Rights of Action

Depending on the circumstances, in addition to any other compensation judged necessary given the situation[91], the court may award damages[92], an injunction[93], or compensation for loss of profits[94]. Note that the court is not required, when evaluating the damages relating to an action for invasion of privacy, to take into account an order to compensate for loss of profit[95]. Finally, the court may order that the defendant must deliver to the person concerned documents which have come into the defendant's possession due to or as a consequence of the violation of privacy[96]. The rights of action granted under this legislation are in addition to other rights of action which may exist[97]. The legal provisions relating to the granting of compensation also present no obstacle to the awarding of any other compensation, claimed in other actions instituted on the basis of acts, conduct or publications which could give rise to an action for invasion of privacy under present law[98].

---

[91] *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 7 (e). *An Act Respecting the Protection of Personal Privacy* R.S.N. c. P-22 s. 6 (1) (e).

[92] *An Act Respecting the Protection of Personal Privacy* R.S.N. c. P-22 s. 6 (1) (a). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 7 (a). *The Privacy Act*, R.S.M. c. P-125 s. 4 (1) (a).

[93] *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 6 (1) (b). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 7 (b). *The Privacy Act*, R.S.M. c. P-125 s. 4 (1) (b).

[94] *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 6 (1) (c). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 7 (c). *The Privacy Act*, R.S.M. c. P-125 s. 4 (1) (c).

[95] *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 6 (1) (c) and s. 6 (2). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 8 (2). *The Privacy Act*, R.S.M. c. P-125 s. 4 (1) (c) and s. 4 (3).

[96] *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 6 (1) (d). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 7 (d). *The Privacy Act*, R.S.M. c. P-125 s. 4 (1) (d).

[97] *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 7 (1). *An Act respecting the Protection of Privacy*, R.S.S. c. P-24 s. 8 (1). *The Privacy Act*, R.S.M. c. P-125 s. 6.

[98] *An Act respecting the Protection of Privacy* R.S.S. c. P-24 s. 8 (2). *The Privacy Act*, R.S.M. c. P-125 s. 6. *An Act Respecting the Protection of Personal Privacy*, R.S.N. c. P-22 s. 7 (2). Note that none of these details are present in the British Columbia legislation.

In Civil Law

The Québec *Civil Code* provisions regarding privacy read as follows:

> Art. 35. Every person has a right to the respect of his reputation and privacy.
>
> No one may invade the privacy of a person without the consent of the person or his heirs unless authorized by law.
>
> Art. 36. The following acts, in particular, may be considered as invasions of the privacy of a person:
>
> (1) entering or taking anything in his dwelling;
>
> (2) intentionally intercepting or using his private communications;
>
> (3) appropriating or using his image or voice while he is in private premises;
>
> (4) keeping his private life under observation by any means;
>
> (5) using his name, image, likeness or voice for a purpose other than the legitimate information of the public;
>
> (6) using his correspondence, manuscripts or other personal documents.

Finally, the *Code* states a general regime on the gathering of personal information and the making of files on other people. These general application provisions are complemented by a specific law governing the gathering, management and communication of personal information by enterprises[99].

The concept of privacy changes according to the context, the period, the habits and values, and, especially, the people involved. It is possible to define its scope: it has two aspects, one regarding identification, the other regarding the context. The identification aspect allows the elements traditionally recognized by the society as included in the domain of a person's privacy, at a given time, to be identified. The contextual aspect allows the content of this domain to be evaluated in terms of the circumstances, in particular of the participation of the individual in society.

---

[99] This is the *Act Respecting the Protection of Personal Information in the Private Sector*, s. Q. 1993, c. 17. The concept of enterprise is defined in the following way in Section 1525, *CCQ*: "The carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service, constitutes the carrying on of an enterprise."

In order to determine whether there has been an invasion of privacy, it is necessary to determine if a disclosure of information or an intrusion affects an element of privacy. This explains the need to try to identify the domain of privacy. The domain of privacy brings together certain types of information belonging to it, in principle. There are also variations depending on the aspects and status of the person involved.

Traditionally, two major aspects of privacy are identified. One is objective and refers to the facts and aspects of a person's life which are included in a protected domain. However, the concrete content of this domain varies from person to person, depending on various circumstances, such as the position one holds in society. This is the subjective aspect of privacy: that which takes the individuals targeted into consideration[100].

Supposing *a priori* that privacy is in opposition to public life, it is indeed possible to identify certain objective elements referring to the private life of an individual which are frequently linked to privacy: health, the privacy of the home, anatomy and privacy of the body, marital and love life, social and political aspects of personality and professional life. These elements can generally be used to specify a person in certain aspects of his or her identity.

With respect to the contextual aspect, the protection granted to privacy varies in accordance with certain values such as time and space. Considering *a priori* that what does not fall into the domain of privacy belongs to that of public life, what seems today to be part of a person's private life could become, over the years or if there is a change in habits and values, public interest information. However, the field of protection of privacy varies mainly depending on the person. Since people do not all play the same roles in society, what might be private information regarding one person will not necessarily be so for another.

For example, the Québec Appeal Court has ruled that although the adulterous relations of a pastor belonged to his private life, the church to which he belonged had not invaded his privacy and had acted with "sobriety and prudence" when it posted a notice announcing his departure and the reasons for it. The Court emphasized [TRANSLATION] "that there are professions that cannot be practised without the public backing of respectable and respected authorities. A person practising such a profession must meet the standards of the supporting authorities or lose their backing"[101].

The contextual aspect of privacy takes into account the situation of persons. Due to the nature of their participation in activities in society, information about certain aspects of the life of certain individuals does not automatically enter into the domain of their private life since the public has a

---

[100] P. A. Molinari and P. Trudel, *supra*, note 12 at 211.

[101] *Église Évangélique Libre du Québec* v. *Vermet*, J. E. 85-75 (C.A.).

legitimate interest in being informed about such facts. This element allows the requirements of public information, and other values which are necessarily in question in the definition of the right to privacy, to be taken into account. The entire issue thus boils down to determining which disclosures are licit and which are not[102].

Pierre Kayser suggests the idea that certain disclosures concerning the private life of certain persons are nonetheless lawful because they are issues about which the public has a legitimate interest in being informed:

> [TRANSLATION] How can the lawfulness of investigations and disclosures relating to public activities and the unlawfulness of those relating to private life be explained? The first fall under freedom of information because the public has a legitimate interest in being informed about them[103].

Since the public's legitimate interest in being informed is one of the fundamental values affecting the scope of the right to privacy, it is logical to think that the domain of the private life of politicians, who must represent the collectivity and manage public funds, will be smaller than that of a simple citizen. The same applies to public persons, as emphasized by Nicole Vallières and Florian Sauvageau:

> [TRANSLATION] The private lives of public persons are of course narrower in scope than those of individuals with no responsabilities to the community. . . . The courts have developed a test to the effect that the conduct of public persons in their private lives cannot be reported or commented on unless that private conduct is of such a nature as to suggest that it will have an impact on the performance of their duties. Facts relating to the private lives of public persons can be disclosed if they are likely to show through or rub off on their public activities. The right to privacy then gives way to the social utility of dissemination of the information[104].

---

[102] P. A. Molinari and P. Trudel, *supra*, note 12 at 215.

[103] Pierre Kayser, *La protection de la vie privée et des autre biens de la personnalité* (Brussels: Bruylant; Paris: LGDJ) at 163.

[104] Nicole Vallières, *supra*, note 39 at 99 ff. See also Nicole Vallières and Florian Sauvageau, *Droit et journalisme au Québec* (Québec: Éditions GRIC - FPJQ, 1981) at 40 ff. Regarding the domain of the private life of public personalities, see also *Bouchard* v. *Chartier* [1907] 31 C.S. 535; *Vigeant* v. *Poulin* [1890] 20 R.L. 567.

Likewise, the state of health of a simple citizen does not have, *a priori*, the same interest in the eyes of the public as that of a celebrity[105] or a public person, as the Court emphasized in the *Valiquette*[106] case. However the private life of a simple citizen could also, under certain circumstances, be revealed, as is shown by Nicole Vallières who notes that jurisprudence has adopted a wide interpretation of the public interest:

> [TRANSLATION] If an individual's private conduct affects interests within the public domain, such as justice, military security and the use of public moneys, or infringes the rights of a social group, that conduct, which is now of general interest, can be debated publicly in the media[107].

Thus, the *contextual* aspect of the definition of privacy is determined by taking into account the requirements of public information as well as the other values which necessarily come into play in the delimitation of the right to privacy. This aspect cannot be defined except through the concrete examination of the position occupied by the subject within society, his or her role in the unfolding of public affairs, the interest members of the public have in knowing certain aspects of his or her behaviour, and the habits and values which could shed light on the decisions and choices they must make with respect to him or her[108]. In sum, the contextual aspect ends up merging with the principal limitations on privacy.

Principal Limitations on Privacy

Privacy cannot be recognized as absolute. Some authors, such as Nadeau and Nadeau, have noted that the limit of a given right is often the limit of another right. [TRANSLATION] "My right ends where another person's right begins. Rights and duties are correlative. The quid pro quo for one person's rights consists in his or her duties relating to another person's right."[109] The limits most likely to be encountered in the Internet are those following from consent, freedom of

---

[105] For a study of the law regarding the image of celebrities, see Susan H. Abramovitch, "Publicity Exploitation of Celebrities: Protection of a Star's Style in Québec Civil Law" (1991) 32 C. de D. 301.

[106] *Valiquette* v. *Gazette (The)**, [1991] R.J.Q. 1075, 1080.

[107] Nicole Vallières, *supra*, note 39 at 98.

[108] Pierre Trudel, "Les dispositions sur la protection de la vie privée dans le nouveau *Code civil* du Québec" (1994) Legipresse no. 111, at 6-7.

[109] André Nadeau and Richard Nadeau, *supra*, note 46 at 228.

expression, the press and other means of communication, maintenance of public order, public interest in information and the absence of reasonable expectations of privacy.

Reasonable expectation of privacy is a notion which was initially developed by the United States Supreme Court in an invasion of privacy case based on the Fourth Amendment[110]. In *Hunter*[111], and especially in *Dyment*[112], the Supreme Court of Canada kept this approach in mind as it incorporated the reasonable expectation of privacy into Canadian constitutional law. Thus, the existence of a reasonable expectation of privacy must be shown in any court action involving the right to privacy.

Respect for privacy in electronic environments seems to tend to be shaped by recognition of the right to anonymity and the right to control over personal information. Since electronic environments presenting many specific situations provide a potential opening for invasion of privacy, it appears that privacy should be protected in accordance with the legitimate expectations of network users, while taking into account the fact that the latter, who are involved to varying degrees in their community life, also have a public life. Since electronic environments are made up, like physical environments, of public and private places[113], the reasonable expectation of privacy should thus vary depending on the context in which the user is situated.

---

[110] See also in this respect *Katz* v. *United States*, 389 U.S. 347 (1967).

[111] *Hunter* v. *Southam* [1982] 2 S.C.R. 145.

[112] *R.* v. *Dyment* [1988] 2 S.C.R. 417. The *Dyment* decision even recognized an information aspect of the right to privacy. In this respect, see: Karim Benyekhlef, *supra*, note 47.

[113] Anne Wells Branscomb writes regarding this: "Is there any place in the Networld that is private? One does not need to be a sexist or a racist to wonder where one must go to bare one's soul to one's friends. [...] There are many other uses for private spaces on educational networks, even networks supported by public funds. Examples include the discussion of the potential appointees, promotions, and student grades. It seems clear that separate cyberspaces should be demarcated for public or private use and that the differences between them must be recognized. Some physical spaces, including designations owned by public entities, are recognized as closed to public discourse; there should be no constitutional barrier to providing private electronic spaces in which confidential exchanges may take place. On the other hand, private spaces are sometimes held to have assumed the role of the state by opening themselves to public access and thus providing a public function. In order to avoid confusion, a cyberspace needs to be clear whether it is a private forum or a public forum." See: Anne Wells Branscomb, "Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspace" (1995) 104 Yale L.J. 1639, 1655.

It has been ruled that certain forms of communication do not carry a reasonable expectation of privacy. In *Smyth* v. *Pillsbury Co.*[114], the judge decided that:

> ...unlike urinanalysis and personal property searches, we do not find a reasonable expectation of privacy in e-mail communication voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once the plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.

Thus, the various Internet contexts do not entail the same expectations of privacy and it cannot be taken for granted that the right to privacy can be invoked each time information is put into circulation. In other words, the manner in which the various responsibilities relating to privacy are defined goes beyond the simple invasion of privacy on the basis of liability. However, the difficulties in identifying the liability of the various Internet actors remain just as great when we attempt to determine who has the burden of ensuring that the privacy of each person is protected.

Protection of Personal Information

Denis Kratchanov notes that "The definition of the right of privacy as the right to exercise some measure of control over information about oneself has led most countries of Western Europe to adopt what is now referred to as data protection legislation. With respect to the public sector at least, the United States and Canada have done so as well."[115]

There is a distinction between protection of the right to privacy and protection of personal information. One is not necessarily the mirror image of the other. The right to privacy has wider implications than does the notion of personal information. This nuance is important in the Internet[116]. In this respect, Benyekhlef writes that:

> [TRANSLATION] The variety of functionalities on the information highway helps us appreciate the diversity and the unequal seriousness of the possible invasions of privacy.

---

[114] 914 F Supp. 97 (1996), http://www.law.uh.edu/faculty/ ECavazos/smyth.html.

[115] Denis C. Kratchanov, *Personal Information and the Protection of Privacy*, prepared for the Uniform Law Conference, June 1995 at 8-9.

[116] Karim Benyekhlef, "Les normes internationales de protection des données personnelles et l'autoroute de l'information" in *Le respect de la vie privée dans l'entreprise, Actes des Journées Maximilien Caron* (17 March 1995), unpublished document, manuscript version, at 38.

> On this subject, the right to privacy must be distinguished from the protection of personal data. The former encompasses the latter. In other words, the protection of personal data is merely a subset of the right to privacy. The fundamental principles of the management of personal information give practical expression to the concerns relating to the informational dimensions of the right to privacy[117].

The fundamental principles regarding personal information management make up the structure of international personal data protection instruments, such as the *OECD Guidelines*, the *European Agreement* and the *Directive of the European Commission* and also national legislation such as the *Act Respecting the Protection of Personal Information in the Private Sector*[118]. These principles are the following[119]: social justification, limited number of subjects gathered, nature of data, specification of goals, limited use, security guarantees, transparency, limited time for data preservation, liability, and individual participation. Failure to respect such principles could give rise to civil liability.

These principles are particularly pertinent with respect to the management of information generated by various electronic tools compiling information on branches, sites visited and use habits of individuals served by Internet access providers (logs). They apply to enterprises conducting business in Québec since in that province the *Act Respecting the Protection of Personal Information in the Private Sector*[120] restates and makes explicit the principles promoted by the OECD. Thus, when personal information is gathered, there must be a serious, legitimate interest in compiling such a file, the purpose of the file must be specified, the information must be from the person specified, the information must be only that required for the file, the person concerned must be notified of the purpose of the file, of its use and of the categories of persons having access to it, and the person concerned must be informed of the location in which the file will be kept and of his or her rights to access and correct the file.

The holding, use and communication of personal information must be protected by adequate security and confidentiality measures. When information is used for a purpose other than that

---

[117] *Ibid*. at 36. See also: Joel R. Reidenberg, "Setting Standards for Fair Information Practice in the U.S. Private Sector" [1995] 80 Iowa L. Rev., forthcoming.

[118] R.S.Q., c. P-39.1.

[119] On these principles in particular and on the protection of personal information in general, see the excellent work by Karim Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'information* (Montréal: Éditions Thémis, 1992.

[120] R.S.Q. c.P-39.1.

mentioned in the file, or when the goal of the file has been attained but the information is to be used again, the consent of the person concerned must be obtained.

Erroneous Information

Article 1457 of the Québec *Civil Code*, in Québec like the common law in the other provinces, creates a duty to be prudent and diligent in the transmission of information[121]. The communication of erroneous information in the framework of a professional activity can be a quasi-offence, even if the information was provided free of charge[122]. Thus, as Barry Sookman explains,

> In the case of negligent provision of information, it is now established that if, in the ordinary course of business or professional affairs, a person seeks information from another, who is not under a contractual or fiduciary obligation to give the information, in circumstances in which a reasonable man so asked would know he was being trusted, or that his skill or judgement was being relied on and the person asked chooses to give the information without so clearly qualifying his answer as to show that he does not accept responsibility, then the person replying accepts a legal duty to exercise such care as the circumstances require in making his reply[123].

Moreover, it seems that the courts tend to be more severe with this type of service, sometimes going even so far as to impose no-fault liability[124]. A current in French doctrine considers that the level of requirement concerning the reliability of information provided differs depending on

---

[121] Barry B. Sookman, "The Liability of Information Providers in Negligence" (1989) 5 Computer Law and Practice, 141-146.

[122] L. Sabater-Bono, "Banques de données: la responsabilité des informations" (1987) Expertises No. 98/99, 309 at 314.

[123] Barry B. Sookman, *supra*, note 121, 141 at 142. See also Heather Black, "Responsabilité en matière d'édition électronique" (Department of Justice of Canada) http://canada.justice.gc.ca/Conferences/Justice_AE/black_fr.html.

[124] J. Huet, "Liability of Information Providers: Recent Developments in French Law Contrasted with Louisiana Civil Law of Liability and United States Common Law of Torts" (1990) 5 Tulane Civil Law Forum, 101 at 114; Affaire Galande, Trib. gr. inst. de Paris, 24 April 1984, D.1985. I. R. at 47 obs H. Maisl, REV. TRIM. DR. CIV. 1984.517, obs. J. Huet: an electronic service which transmitted erroneous information to companies, *without however having been proven to have done so negligently*, was ordered by the court to interrupt its service until its data had been completely rectified.

whether what is in question is professionalor general-public computer-based communications[125]. The trend is thus to distinguish between public communications services, which resemble existing mass media, and the specialized information services which fulfil the needs of professionals[126].

Access to communications services intended for the general public is provided with no prior contract between the information producer and the user[127]. Such data banks have an obligation to be prudent and diligent when they transmit information[128]. If the service is negligent and transmits erroneous information, it will then be held liable for damages[129].

Access to professional data banks is regulated by the conclusion of a model contract[130]. The courts demonstrate a tendency to be more severe regarding this type of service, even going so far as to impose no-fault liability[131].

In the United States, the courts require more than simple negligence to hold the traditional media liable for the transmission of erroneous information outside of a contractual framework[132]. A

---

[125] X. Linant de Bellefonds and A. Hollande, *Droit de l'informatique et de la télématique* (Paris: J. Delmas et Cie., 1990) at 128.

[126] J. Huet, *supra*, note 124 at 113.

[127] L. Sabatier-Bono, *supra*, note 122 at 309.

[128] J. Huet, *supra*, note 124 at 115. See also: Affaire Polac., Trib. gr. inst. de Paris, 29 January 1986, D. 1986, flash, No. 10.

[129] J. Huet, *supra*, note 124 at 117. See also: Affaire de "La cigue", Trib. gr. inst. de Paris, 28 May 1986: the author and the publisher of a cook book were held liable for having negligently transmitted information on a plant, which lead to the poisoning of a reader.

[130] L. Sabatier-Bono, *supra*, note 122 at 309.

[131] J. Huet, *supra*, note 124 at 114. See also: Affaire Galande, Trib. gr. inst. de Paris, 24 April 1984, D.1985. I. R. at 47 obs H. Maisl, REV. TRIM. DR. CIV. 1984.517, obs. J. Huet: an electronic service which transmitted erroneous information to companies, *without however having been proven to have done so negligently*, was ordered by the court to interrupt its service until its data had been completely rectified.

[132] *Jaillet* v. *Cashman*, 115 Misc. 383, 189 N.Y.S. 743 (1921), aff'd, 202 App.Div. 805, 194 N.Y.S. 947 (1922), aff'd, 235 N.Y. 511, 139 N.E. 714 (1923); *Gutter* v. *Dow Jones, Inc.*, 490 N.E.2d 898 (Ohio 1986); *Gale* v. *Value*

Court recently applied this principle to electronic means of communication and did not hold an information provider responsible for the transmission of false news[133].

Liability for the transmission of erroneous information, in an extra-contractual situation, is affected in part by the importance of the information for the receiver and the use he or she is likely to make of it. Even in the absence of a contractual relation, a person who claims to be an information provider can be held responsible for damages suffered by a person who depends on that information[134].

In *87118 Canada Ltd.* v. *The Queen*[135], the obligation for an electronic information system to act with prudence and diligence was recognized by the Federal Court. In that case, the defendant was granted compensation following damages suffered after the computer system failed to indicate that the corporate name the defendant was about to choose already existed.

The possibility of ensuring error-free transmission of information, the costs that such transmission would entail, and the reliability of the written documents which the computerized system must replace are also factors which should be taken into account. In *87118 Canada Ltd.*, the Court suggested that a computerized system intended to replace a manual one should be at least as reliable as the latter, no matter what could be reasonably expected given the state of knowledge and the state of technological knowledge at the time the error was committed[136]. A New York court has asserted, regarding this, that the failure of a computerized system to use new technological tools which could improve its service could be considered to be negligence if damages result[137].

Line, Inc., 640 F.Supp. 967 (D.R.I. 1986); *First Equity* v. *Standard & Poor's Corp.*, 670 F.Supp 115 (S.D. N.Y. 1987), aff'd, 869 F.2d 175 (2nd Cir. 1989).

[133] *Daniel* v. *Dow Jones & Co. Inc.*, 520 NYS 2d 334 (NY Sup.Ct 1987).

[134] Blodwen Tarter, "Information Liability: New Interpretations for the Electronic Age" (1992) 11 Computer Law Journal 481, 497.

[135] *87118 Canada Ltd.* v. *R.*, 53 CPR (2d) 177, rev'd 56 CPR (3d) 209 (Fed.CA) (1981).

[136] Barry B. Sookman, *supra*, note 121 at 143.

[137] *Swiss Air Transport company* v. *Benn*, 467 NYS 2d 341 (NY City Civ. Ct. 1983).

As for the type of information transmitted, French doctrine holds, for example, that if the computerized data bank simply stores whole documents or is made up only of abstracts or summaries from source documents, then the system operator has obligations only regarding means[138].

Regarding the transmission of erroneous information, some authors believe that no-fault liability should be imposed on the editor of the publication, that he or she should be held responsible whenever the information is inexact, and that there should be no requirement of evidence that he or she committed a fault and no possibility of exoneration even if it can be proven there was no fault on his or her part, but that the error results from a third party[139].

Some[140] consider that a service provider which transmits erroneous information leading to damages can be held responsible under the manufacturer's liability regime. Some believe that the rules stated in Article 1468 of the *Civil Code* provide for no-fault manufacturer's liability when the product does not meet normal safety criteria[141]. Others however claim that the *Civil Code* states a presumption of knowledge of the defect by the manufacturer; but, that the latter can avoid liability by demonstrating reasonable diligence[142].

---

[138] L. Sabatier-Bono, *supra*, note 122 at 316.

[139] Jean Beauchard, "Communicatique et responsabilité civile" in *Le droit de la communicatique* (Montréal: Éditions Thémis, 1992) 117 at 127.

[140] Jay R. McDaniel, "Electronic Torts and Videotext - At the Junction of Commerce and Communications" (1992) 18 Rutgers Computer & Technology Law Journal, 773 at 830.

[141] W. E. Crawford, "Manufacturer's Liability under the Proposed Revision of the *Civil Code* of Québec" in Institut canadien d'études juridiques supérieures, *Conférence sur le nouveau Code civil du Québec* (Cowansville: Éditions Yvon Blais, 1992) 415 at 422; J. Dennis, "Basic Principles of Manufacturer's Liability under the Civil Code of Québec" in Institut canadien d'études juridiques supérieures, *Conférence sur le nouveau Code civil du Québec* (Cowansville: Éditions Yvon Blais, 1992) 403 at 409.

[142] Jean-Louis Baudouin, *supra*, note 32 at 1156.

In any case, manufacturer liability supposes the presence of a defective good or product[143]. We must thus ask whether information is a product[144]. In the American case of *Jan Way* v. *Boy Scouts of America*[145], the court refused to hold a magazine liable for the distribution of erroneous information under the regime of manufacturer liability. The court considered that this regime applied to defective tangible products, but that, according to it, words and ideas did not fall into that category.

In a specific instance in the United States, the court applied no-fault product liability in the case of an airplane accident caused by an aerial map which included incorrect data provided by the Federal Aviation Agency[146]. Extremely technical information was, in this case, judged to be a product. Manufacturer liability appears to be applicable to those who distribute highly technical information, but the courts have refused to extend this same liability to manufacturers of newspapers, books and periodicals with a wider range and intended for the general public[147].

In Canada until now, the Supreme Court has refused to consider information to be like a good since it cannot be the subject of property rights[148]. The Supreme Court recognizes however that if the information is part of a tangible thing (for example, if it is found on a diskette), then it can be considered to be a good[149]. This could perhaps allow the application of the theory held by those who consider that if information is distributed through a medium which has the appearance of a product (for example, a CD-ROM), then manufacturer liability comes into play[150].

---

[143] Art. 1468, *Québec Civil Code*.

[144] Lawrence Savell, "Who's Liable when the "Product" is Information" (28 August 1993) Editor & Publisher 19 at 19.

[145] Texas Appeal Court, 13 May 1993, jurisprudence cited in Lawrence Savell, *supra*, note 144 at 19.

[146] *Brokles-By* v. *United States*, 9th circuit decision, 1985.

[147] Lawrence Savell, *supra*, note 144 at 35.

[148] *Wayne John Stewart* v. *R.* [1988] 1 S.C.R.

[149] *Wayne John Stewart* v. *R.* [1988] 1 S.C.R.

[150] J. Huet, *supra*, note 124 at 125.

Violation of Secrecy

Violation of secrecy is considered an offence in both common and civil law. Under both systems, causing damages by breaking a relation of confidentiality is viewed as a wrongdoing subject to sanction.

In Common Law

The penalty for violation of secrecy is partially ensured in common law by the tort of Breach of Confidence. Courts base their jurisdiction in this matter on the duty of each individual to act in good faith. In *Fraser* v. *Evans*[151], the British Court of Appeal wrote:

> No person is permitted to divulge to the world information which he has received in confidence, unless he has just cause or excuse for doing so. Even if he comes by it innocently, nevertheless once he gets to know that it was originally given in confidence, he can be restrained from breaking that confidence. But the party complaining must be the person who is entitled to the confidence and to have it respected. He must be a person to whom the duty of good faith is owed[152].

The limitations on the right to oppose the divulgence of secrets follow from the consent of the party concerned or from circumstances in which public interest is stronger than the necessity to protect the secret. However, as Peter Burns points out, because it is a right which "has tended to develop within the confines of the courts' discretionary role in granting injunctions, its limits are difficult to delineate"[153].

In Civil Law

When a person is held to a duty to preserve the secrecy of information, revealing such information is a fault and entails liability.

For example, Article 2088 of the *Civil Code* provides that:

---

[151] [1969] 1 Q.B. 349 (C.A.) Per Lord Denning.

[152] [1969] 1 Q.B. 349 (C.A.) Per Lord Denning at 361.

[153] Peter Burns, *supra*, note 48 at 39.

> Art. 2088. The employee is bound not only to carry on his work with prudence and diligence, but also to act faithfully and honestly and not to use any confidential information he may obtain in carrying on or in the course of his work.

Regarding trade secrets, the code specifies the precise type of compensation which is due when there is a violation of the duty of confidentiality. Article 1612 provides, in effect, that:

> Art. 1612. The loss sustained by the holder of a trade secret includes the investment expenses incurred for its acquisition, perfection and use; the profit of which he is deprived may be compensated for through payment of royalties.

Unfair Competition

Competition is legitimate in our economic system, but if it becomes deceitful or otherwise ceases to be fair and honest, it is actionable and thus makes liable those who engage in it.

In Civil Law

Unfair competition which causes unjust harm to another is governed by civil liability. Such competition is contrary to the honest practices of industry and business[154]. The courts require that there be an element of bad faith or an intention to cause harm in order to conclude that they are faced with an instance of unfair competition. In *Corbeil* v. *Dufresne*[155], the judge defined the fault of unfair competition as [TRANSLATION] "an act committed in bad faith that creates confusion between the products of two manufacturers or merchants or that, while not creating confusion, casts discredit on a competitor." Nadeau and Nadeau agree that the notion can cover many different forms of action, such as the substitution of products, counterfeiting, blatantly false advertising, theft of secrets, and usurpation of a sign or acronym.

In Common Law

Common law does not contain the general category of unfair competition, but it does provide a certain number of means of recourse covering most of the circumstances or activities, which are usually linked with such a category.

---

[154] André Nadeau and Richard Nadeau, *supra*, note 46, no. 205.

[155] *Corbeil* v. *Dufresne* (1933) 71 C.S. 548.

Action for passing off aims at curbing the sale of merchandise and the conduct of business which leads members of the public to falsely believe that the merchandise or business is that of another person[156].

Action for injurious falsehood punishes inaccurate statements knowingly made in order to damage the business interests of others. The field of recourse differs from that of defamation, which protects personal reputation, in conjunction with the person's economic interests.

The plaintiff must establish that the statements made were inaccurate, that they were made with malice and that they caused damages.

---

[156] *Salmond on Torts* (1957) at 659.

3. Actors and Responsibilities

While it is generally easy to accept that the individual who personally committed the justiciable action is responsible for the resulting damages, the Internet context raises important questions regarding the responsibilities of those who intervene in the transmission of messages and in the provision of an environment making communications possible.

In order to shed light on the legal situation of these various actors in Internet communications, it is useful to employ metaphors in order to analyze the factors which should be considered in the evaluation of their liability.

The Principal Metaphors

The law establishes frameworks for new phenomena using analogies with known situations. Present law already contains a set of principles intended to regulate broadcasting and the exchange of information. The goal of legal research is to identify precisely how these principles apply to novel situations. This task is often made easier through the use of metaphors, such as that of a highway, which allow the identification of analogies and possible legal regimes[157].

In many situations in which damage results from information circulation, the criteria for assigning liability take into account the roles assumed by the various participants in the process of the assignment of value to information: publisher, simple carrier, broadcaster, newspaper, etc., for the duties and responsibilities linked to each of these roles are well established in liability law.

Thus by extrapolating both from the characteristics which are presented by the various communications contexts found on the Internet and from the analogies demonstrated by the roles and functions of the various actors, it is possible to determine who is responsible for the damage resulting from the transmission of information on the Internet.

Recourse to such a procedure has a significant advantage: it facilitates the establishment of lines of reasoning which can be used to apply legal principles. However, metaphors must be used carefully. The roles played in traditional communications contexts are not always found on the Internet; and, on the Internet, they can have completely new dimensions. Cutera notes that "the legal system is trying to fit square pegs into round holes"[158]. Branscomb believes it would be

---

[157] David R. Johnson and Kevin Marks, *supra*, note 1 at 487; Henry H. Perritt Jr., "Metaphors for Understanding Rights and Responsibilities in Network Communities: Print Shops, Barons, Sheriffs and Bureaucracies - Discussion Paper" posted in "information Law Papers", Villanova University Server.

[158] Terri A. Cutera, "Computer Networks, Libel and the First Amendment," (Dec. 1992) 11 Comp./L.J. 555 at 581.

imprudent not to take into account the various modes of information transportation which can be represented by a single actor:

> Imposing legal metaphors [...] would be unwise without differentiating the ways in which these providers represent different modes of information transport, not all of which have real-world counterparts.[159]

The analogical approach rests on comparisons to functions prevailing in the universe of communications which could lose ground with the convergence of technologies. Johnson and Marks consider that such an approach fails to take into account qualities inherent to cyberspace:

> These attempts [...] presuppose that there is a "best fit", some metaphor that will accurately characterize all the activities involved in these systems. In fact, the most significant attribute of "Cyberspace" is its malleability, the ability to change to fit a variety of metaphors.[160]

It is useful nonetheless to refer to such analogies in order to better grasp the essence of present rules and to illustrate the presence of factors which come under consideration in the determination of the respective liabilities. In order to identify the scope of rights and responsibilities, it is useful to take as examples the liability regimes related to activities analogous to communications in computer networks. Such analogies can be found in domains such as those of the transportation and distribution of printed matter.

We will note that there is a close link between the control exercised over information presumed harmful and the liability which follows from it. Thus, the greater the discretion to make decisions on what is to be published (transmitted), the greater the liability implied by such decisions[161].

With respect to the circulation of information, several kinds of roles are assumed in the Internet, each of which has variations and combinations entailing that in certain situations a single entity may assume more than one role. In any case, in open network environments, there are invariably system operators, information providers, among which there are users and one or more information carriers. What magnifies the impression of a so-called "legal vacuum" regarding the Internet is the absence of consensus on the metaphors which should aid in situating the roles of

---

[159] Ann W. Branscomb *supra*, note 114.

[160] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 488.

[161] Joseph P. Thornton, Gary G. Gerlach and Richard L. Gibson, "Libel (Symposium: Legal Issues in Electronic Publishing)" (Sept. 1984) 36 Federal Communications Law Journal 178-181.

the participants in electronic communications and, in many respects, the inability of each of the metaphors to portray the roles which are effectively performed in computer communications.

The Publisher

A publisher publishes information. To publish means to communicate information to third parties knowing that the information will be read, seen or heard. Voluntary publication supposes knowledge of the content of the information transmitted[162]. In the Internet context, publication can result from the transmission of files, from discussion in the framework of electronic conferences, or from making available information in files which can be transferred through the network[163].

In all of these situations, there is one constant: the decision to publish belongs to the publisher. For this actor, this is an option: there is no obligation to publish. In the world of the press and publishing, it is normal to hold that the director of publishing is able to control the information which circulates due to his or her enterprise[164]. From such controlling power follows liability for the transmission of harmful information.

However, as some authors have remarked, it is doubtful whether this presumption is always verifiable on the Internet, especially in situations in which there is no "fixing prior to the communication to the public", which is the only way for a site operator to exercise any control[165].

This is a limitation on this metaphor regarding electronic environments because to ask site operators to effectively supervise the content of everything they transmit to the public supposes a considerable burden[166]. This leads to attention being removed from the intention to broadcast and

---

[162] Loftus E. Becker, Jr., "The Liability of Computer Bulletin Board Operators for Defamation Posted by Others" (Fall 1989) 22 Connecticut Law Review, 203 at 217.

[163] Timothy Arnold-Moore, "Legal Pitfalls in Cyberspace: Defamation on Computer Networks" (1994) 5(2) Journal of Law and Information Science 165 at 178. (http://www.kbs.citri.edu. au/law/defame.html).

[164] David R. Johnson and Kevin A. Marks, *supra*, note 1, at 492.

[165] X. Linant de Bellefonds and A. Hollande, *supra*, note 125 at 131.

[166] David R. Johnson and Kevin A. Marks, *supra*, note 1, at 492. See also Edward A. Cavazos, "Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability for a new Technology" (Fall 1992) 12 Review of Litigation 231 at 238.

placed on the intention to communicate a message *of which the site operator should have known* the harmful nature[167].

In *Stratton Oakmont Inc.* v. *Prodigy Services Co.*[168] the court concluded that the Prodigy network had assumed the role of a publisher. A subscriber to Prodigy had sent a defamatory message concerning the President of Stratton onto the network. The court held Prodigy responsible for the damage caused.

In order to decide to call Prodigy a publisher, the court examined the behaviour of the site operator with respect to information carried. In this case, Prodigy exercised a degree of control over the information: it was reputed to answer for the information it transmitted because it was supposed to be aware of the content[169].

From this decision, many concluded that when a site operator claims to offer a service free of "vices", adopts a code of conduct, pays employees to ensure such a code is respected, and provides an arbitrator for cases of conflict regarding certain statements, then the site operator makes itself liable for the content carried by its services. By assuming the same control as that of a publisher, the site operator also takes on the same liability[170]. Against such a conclusion, some have argued that by declaring the service to be a "family" service, Prodigy played the role of a bookseller which chooses the type of literature it wishes to sell, but that such choice does not make it a publisher[171].

---

[167] Jay R. McDaniel, *supra*, note 140 at 817-818.

[168] Index No. 31063/94, N.Y. Sup. Ct., 24 May 1995.

[169] David Loundy, "Holding the Line, On-Line, Expands Liability" (8 June 1995) Chicago Daily Law Bulletin at 6.

[170] *Ibid.*

[171] Eugene Volokh, cyberia-1@listserv.cc.wm.edu, 11/07/95, 21:46, FYI, re: Stratton Oakmont v. Prodigy.

Nonetheless, it remains that editorial control is recognized when a participant in electronic communications[172]:

> - examines messages and exercises control over their contents before they are transmitted;
> - deletes messages or actions of users which do not fulfil the criteria he or she has determined.

It is appropriate, however, to distinguish cases in which the site operator, in order to prevent a discussion group from overflowing out of the theme it is assigned, does not allow certain off-topic messages. The site operator is then not automatically considered to be a publisher. This is due to the simple fact that its target is not editorial control over the content so much as a restriction of content to a certain zoning in the network[173].

The Broadcaster

When they are free to broadcast, broadcasters are generally considered to be the publishers of the statements they transmit and thus to have the same standards of liability as the latter. The written press, the radio and TV are subject to the provisions of the principles of civil liability except if a statutory exception suspends or modifies their application.

Broadcaster liability can result from harmful statements made by members of the public acting in their own names. In this respect, the general rule governing broadcaster liability remains the same if it can be proven that all measures to prevent harmful statements had been taken[174]. In this respect, a Canadian court has refused to apply the American doctrine of the "outside speaker" which makes the broadcaster responsible for the statements of an "outside guest speaker" except in so far as evidence is established that the broadcaster was negligent[175].

---

[172] Eric Schlachter, *supra*, note 6 at 135.

[173] *Ibid*. [Since all users have the opportunity to post messages as they wish, many discussion groups can easily become invaded by "junk postings" if the "sysop" does not withdraw unrelated messages.]; Henry H. Perritt Jr., "Tort Liability, the First Amendment and Equal Access to Electronic Networks" (1992) 5 Harvard Journal of Law & Technology 65 at 140. [A network could not survive if every single individual could publish whatever he or she desired and evaluate the content of his or her messages in accordance with his or her own system of values.]; Edward A. Cavazos, "Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability for a New Technology" (Fall 1992) 12 Review of Litigation 231 at 239. [A discussion group which addresses itself to children should not contain messages "for adults only".]

[174] Pierre Trudel and France Abran, *Droit de la radio et de la télévision* (Montréal: Thémis, 1991) at 464.

[175] *Lawson* v. *Burns, Succamore and Jim Pattison Broadcasting Ltd*, [1976] 6 W.W.R. 362 (B.C.S.C.).

The rule which applies in Québec is similar to that which is advocated by a certain current in French jurisprudence, which holds that in spite of the fact that the broadcaster's liability cannot result directly from the statements of a member of the public which are transmitted "live", it does result from the "authorization" to speak which the broadcaster accords that person[176]. The Paris Court of Appeal asserted however that a broadcaster is liable for the statements of a member of the public which are transmitted "live" only if the broadcaster endorses them or if the statements are made with the broadcaster's connivance[177].

In certain circumstances, while they may be participants in the publication process, broadcasters may not be able to intervene in the content of the information broadcast. For example, press operators (for a newspaper), couriers which carry the publication and radio or television engineers have no control over content[178]. In general the secondary publisher does not know the content of the information he or she carries and is thus not able to prevent harmful statements from circulating.

The standard of liability thus applied resembles that generally attributable to a carrier, in other words, the case in which there is no liability for the harmful content of the messages transmitted[179]. Moreover, some advocate a presumption that secondary publishers are ignorant of the harmful content of the information. [180]However, the secondary publisher is liable if he or she knew or had reason to know of the defamatory nature of the message transmitted[181]. In such a case, the secondary publisher then becomes a kind of re-broadcaster and acquires the same liability as the latter[182].

---

[176] *Affaire Polac*, Trib. gr. inst. de Paris, 29 January 1986, flash, no. 10.

[177] Paris, 1st Ch. Sect. A, 6 October 1987.

[178] David J. Loundy, "E-law: Legal Issues Affecting Computer Information Systems and Systems Operator Liability" Online 1995 (http"//www.leepfrog.com/E-Law/Contents.html).

[179] Terri A. Cutera, *supra*, note 158.

[180] Robert Charles, "Computer Bulletin Boards and Defamation: Who Should be Liable? Under What Standard?" (1987) 2 J.L. & Tech, 421 at 131; David J. Loundy, *supra*, note 179.

[181] *Lerman* v. *Chuckleberry Pub. Inc.*, 521 F. Supp. 228, 235 (S.D.N.Y. 1981).

[182] David J. Loundy, *supra*, note 178.

The Re-broadcaster

A re-broadcaster circulates material *published by others*[183]. A re-broadcaster's liability is largely determined by the existence of possibilities of verifying the content of the information broadcast.

In principle, individuals who re-circulate harmful information are liable in the same way they would have been if they themselves had written or published it in the first place. Thus, a radio or television station which only broadcasts the statements of a third party and a newspaper which reprints what has been said or written by others are considered to be the primary publishers of such statements and are thus liable for them[184]. A broadcaster which re-circulates defamatory statements, regardless of the source of such statements, even if it is a news agency which the journalist believed to be reliable, is liable for them: it cannot be exonerated[185]. In such situations, it is possible to check the information, or at least to be aware of its possibly harmful nature.

The Librarian

The category of distributor is distinct from that of re-broadcaster. Librarians, like booksellers, are information distributors. In other words, they deliver or provide information whereas a re-broadcaster repeats it[186].

Normally, distributors do not control the content of the information they transmit and are not liable if it is harmful[187]. In effect it would be unthinkable for each distributor (newsstand, book

---

[183] Eric C. Jensen, "An Electronic Soapbox: Computer Bulletin Boards and the First Amendment" (1987) 39 Federal Communications Law Journal 217; Joseph P. Thornton, Gary G. Gerlach and Richard L. Gibson, *supra*, note 161 at 179.

[184] Joseph P. Thornton, Gary G. Gerlach and Richard L. Gibson, *supra*, note 161 at 179; *Cianci* v. *New Times Publishing Co.*, 639 F.2d 54, 61 (2d Cir.1980); *Lerman* v. *Chuckleberry Publishing Co.*, 521 F. Supp. 228, 2335 9S.D.N.Y. 1981); *Macaluso* v. *Mondadori Publishing Co.*, 527 F.Supp. 1017, 1019 (E.D.N.Y. 1981).

[185] *Chinese Cultural Centre of Vancouver* v. *Holt* (1978), 7 B.C.L.R. 81 (S.C.).

[186] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493.

[187] Trotter Hardy, "The Proper Legal Regime for "Cyberspace" (1994) 55 University of Pittsburgh Law Review, 993 at 1003; David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493.

store, library) to have the duty to check the contents of each publication distributed in order to be sure that it contains no harmful information[188].

However, when they are made aware of the harmful nature of information, distributors have the duty to withdraw it. If they do not do so, they can be held liable for the damage caused by such statements[189].

The problem with electronic environments is that the majority of site operators participate in their own systems (without, nonetheless, exercising real control over all the information circulating in it). Such participation could be interpreted, according to some authors, as implying real or presumed knowledge of the harmful nature of the information contained in the system. The site operator who has been informed of the harmful nature of the information would have the obligation to take all necessary measures to prevent the circulation of or to withdraw the information, or else he or she could be held responsible for the harm caused by such information[190]. The site operator's liability would be mitigated, hoever, by the requirement of being attentive to the problematic nature of the information found in a site partially or wholly under its control.

In the Cubby case, an electronic message distributed in CompuServe contained unflattering remarks about a rival server (Cubby). The court concluded that CompuServe had no control over the information circulating in its system and that it could not know or have reason to know of the harmful nature of the messages. It was thus not liable. The court compared CompuServe to an electronic library. Like a library, CompuServe had the choice of circulating a work or not, but once the work was in the system it could exercise no editorial control over it. Moreover, even if CompuServe had wanted to examine each message, the extremely large number of messages would have made such action impossible[191].

According to some, the analysis performed in the Cubby case seems to imply that in order to avoid liability, all the site operator has to do is close its eyes to the information circulating in its

---

[188] *Balabanoff* v. *Fossani*, 81 N.Y.S.2d 732, 733 (Sup. Ct. 1948). American jurisprudence even considers that a law which would impose strict liability on a distributor, for example on a librarian, for the content of the works he or she distributes would be unconstitutional because it would have the effect of indirectly restricting information transmitted to the public (since the works available would be only those inspected by the librarian). See: *Smith* v. *California*, 361 U.S. 147 (1959), reh'g denied, 361 U.S.; Trotter Hardy, *supra*, note 187 at 1003.

[189] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493; David J. Loundy, *supra*, note 178.

[190] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 494.

[191] *Cubby* v. *CompuServe Inc.*, 776 F.Supp. 135 (S.D.N.Y. 1991) at 140.

network[192]. A site operator which knew or should have known that harmful information was being carried in its network and which exercised no control over such information would then become a kind of re-broadcaster and acquire the same liability as the latter[193]. This would require, however, the participation of users who would have to inform the system operator of the existence of information they consider potentially harmful.

Some claim however that, even if they are considered to be like libraries, "sysops" operating less busy systems would have the duty to examine messages since there is the possibility, in an electronic environment, of performing an automatic computer search of words or expressions likely to be harmful (whereas a library in the real world would have to perform such a search manually)[194].

In electronic environments, information storage is not necessarily done by large, easily identifiable storefront publishing companies. Presently, the fact that a librarian or bookseller is not liable for what he or she distributes has little effect on the victim since he or she will attack the publisher of the document directly. In electronic environments, what would happen if the system operator were not liable and the publisher was unknown or insolvent?[195]

Yet, the system operator often lacks a legitimate motive to intervene in order to suppress potentially harmful information. In the name of what and in virtue of what authority must a system operator decide whether a given piece of information is actionable or not? In virtue of what authority should it assume the role of a tribunal charged with determining if the content is harmless or harmful?

The Retransmitter

Programming distributed by broadcasting distribution companies does not originate with those companies. It is received and then transmitted. Thus, direct satellite-to-home broadcasting and cable distribution systems are considered to be like broadcasting distribution companies when the operator acts as a re-transmitter of existing signals. The operator does not produce or order programs and does not modify the content of the programs on any of the signals distributed.

---

[192] Edward A. Cavazos,*supra*, note 166 at 242.

[193] David J. Loundy, *supra*, note 178.

[194] Trotter Hardy, *supra*, note 187 at 1003 (Trotter Hardy agrees however that it is almost impossible to determine "harmful words".)

[195] Trotter Hardy, *supra*, note 187 at 1005.

Such programs can be distributed either coded or uncoded. Multipoint distribution systems are also included in the category of broadcasting distribution companies insofar as the operator neither produces nor orders programs and does not modify the content of the programs on any of the signals distributed[196].

In such situations, re-transmitters cannot be assigned liability for the content thus re-transmitted.

The Owner of a Space

Some have argued that electronic communications sometimes require the use of an individual's property[197]. This leads to the consideration that certain participants sometimes find that presumably harmful information is located in a space they own.

Owners are rarely held liable for acts committed on their property. Timothy C. May compares some system operators to hotels which rent rooms (electronic spaces) to users and which have no obligation, or right, to supervise what the latter do there. They thus have no liability if illegal activities occur there.

This line of argument corresponds to the rule established in Québec jurisprudence which states that a landlord is not necessarily responsible for the misdeeds of his or her tenants[198]. Obviously, a hotel which, with complete awareness, makes itself the centre of illegal activities is liable for damages, as would be a site owner which endorsed defamatory messages transmitted by users[199].

Moreover, it is recognized that an owner who is informed of the presence of harmful statements on the walls of his or her property and who does nothing to remove them, is considered to be a re-broadcaster of those statements and is liable for them to the same extent as the author of the message[200]. Likewise, site operators would always have the duty to withdraw information they

---

[196] CRTC, Public Notice 1987-254 (26 November 1987), Regulatory Policy for Direct-to-Home (DTH) Satellite Broadcasting Systems, Multiple Distribution Systems (MDS), and Subscription Television (STV) Systems.

[197] Timothy C. May, "Who is Responsible on the Net" law.listserv.cyberia-1, (Subject: Cyberspace is more like property, lease space, rent, etc.) 7 February 1995 12:31:21.

[198] *Bissonnette* v. *Corriveau* [1992] A.Q. 2005; *Bissonnette* v. *Boulet* [1992] A.Q. 2004.

[199] Timothy C. May, *supra*, note 197.

[200] *Hellar* v. *Bianco* 11 Cal. App. 2d 424, 244 P.2d 757, 28 ALR2d 451 (1952); *Scott* v. *Hull*, 22 Ohio App.2d 141, 259 N.E.2d 160, (1970); *Tackett* v. *General Motors Corporation*, 836 F.2d 1042 (7th Cir. 1987); *Woodling* v.

know to be harmful if they do not want to be assigned liability as re-broadcasters[201]. According to this metaphor, the prerequisite to liability would be the knowledge of the presence of harmful information in a site[202].

The Carrier

Like a carrier, an electronic communications system sometimes acts only as a conduit for transporting information from one site to another[203]. Carriers are in principle freed of liability for the content of statements they carry for their users[204]. Contrary to publishers and distributors, carriers have the obligation to carry any message and may discriminate neither against the content of the message nor against the person who sends it[205].

Nonetheless a carrier, like a telecommunications company, can be held liable for the content it carries if it is itself the author of the statements: its situation would be that of a publisher. Generally, it acquires no responsibility for content which comes from third parties and which circulates on its lines since it is then simply a conduit[206]. The Ontario Supreme Court decided that in effect it would be unthinkable for each employee of a telegraph company to be responsible for

---

Knickerbocker, 17 N.W. 387 (Minn. 1883).

[201] Eric Schlachter, *supra*, note 6 at 118.

[202] Jay R. McDaniel, *supra*, note 140 at 825.

[203] David J. Loundy, *supra*, note 178.

[204] Michael H. Ryan, *supra*, note 13 at 416; Lynn Becker, "Electronic Publishing; First Amendment Issues in the Twenty-First Century" (1984-85) 13 Fordham Urban Law Journal, 801 at 857.

[205] David R. Johnson and Kevin A, Marks, *supra*, note 1 at 495; Terri A. Cutera, *supra*, note 158 at 555; *Chastain* v. *British Columbia Hydro & Power Authority* [1973] 2 W.W.R. 481; *Telecommunications Act*, S.C. 1993, c. 38, s.36: "Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public."

[206] Floyd Abrams and Dean Ringel, "Content Regulation (Symposium: Legal Issues in Electronic Publishing" (Sept. 1984) 36 Federal Communications Law Journal 153.

checking each message and for deciding if the content is harmful or not[207]. However, common law recognizes that carriers must provide evidence of reasonable diligence in the transmission of messages.

The Supreme Court of Canada distinguishes between messages intended to be published (for example, letters and news for newspapers) from purely personal messages. The Court held telegraph companies liable for the content of messages intended to be published since in such cases it considered the telegraph company to be like a publisher[208]. Others go so far as to believe that there is a presumption that the defamatory statements contained in a telegraph were published through their transmission[209]. According to this reasoning, the telegraph company would be presumed at all times to be playing the role of a publisher and, unless there is proof to the contrary, would be liable for damages. Against this line of thought, some hold that the transmission of messages by carriers never amounts to a publication of the statements and that carriers never have more than a right to limited control over messages[210].

Unlike telegraph companies, telephone companies have never been held responsible for the content of the messages they carry since according to some they do not "transmit" messages[211]. The person speaking is the one who truly transmits the message and he or she is liable for the content[212].

The situation is however different for messages which are recorded and then transmitted by a telephone company (voice mail). In the U.S., a court held that even if a telephone company could be held responsible for having "published" such messages, such a company should be granted a

---

[207] *Kahn* v. *Great Northwestern Telegraph Co. of Canada* (1930) 39 O.W.N. 143 (C.A.).

[208] *Dominion Telegraph Co.* v. *Silver* (1882) 10 S.C.R. 238.

[209] *Pavlovic* v. *Knutson* (30 June 1982) Doc. No. 137/1981 (Sask. Q.B.).

[210] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 495.

[211] Michael H. Ryan, *supra*, note 13 at 416; Bell Canada's Terms of Service, s. 16 (approved by the CRTC) states: "Bell is not liable for [...] defamation arising from material transmitted over its facilities".

[212] *Electric Despath Co.* v. *Bell Telephone Co.* (1891) 20 S.C.R. 83.

privilege and be relieved of its liability[213]. American jurisprudence thus grants extensive immunity to telephone companies[214].

Some believe[215] that comparing electronic environments to actual carriers is not appropriate because of the carriers' obligation to transmit information without discrimination. In *Cubby* v. *CompuServe*[216], the CompuServe network was sued as a co-defendant in a defamation case. This action resulted from information published in an electronic information letter entitled: "Rumorville USA". This information letter was published by a network subscriber who had no other link with CompuServe. Leisure J. exonerated CompuServe, noting that in this case CompuServe did not have the possibility of becoming aware of the information broadcast. The company received no fees for providing public access to the electronic site, just as it paid no fees to broadcast that site to its subscribers.

In so far as CompuServe could not be aware of the harmful nature of the information transmitted, it assumed no liability in that respect.

From this analysis one might infer that it is incumbent on the network operator to do whatever is necessary to withdraw information when it becomes aware of its harmful nature. Such an approach tends to lead to the conclusion that the degree of responsibility of the network operator is closely linked to the degree of control it exercises or is supposed to exercise over the information transmitted or otherwise available on its network.

This demonstrates the crucial importance of qualifying the role played by information providers. Thus, in *Stratton Oakmont* v. *Prodigy*[217], an investment firm sued Prodigy following defamatory statements transmitted on an electronic site broadcast by Prodigy. The court decided that Prodigy exercised some degree of control over the content and ruled in consequence.

---

213 *Anderson* v. *New York Telephone Company*, 320 N.E.2d 647 (N.Y. Ct. App. 1973).

214 Jay R. McDaniel, *supra*, note 140 at 822.

215 Edward A. Cavazos, *supra*, note 166 at 239.

216 *Cubby* v. *CompuServe Inc.* (1991) 776 F. Supp., 135; See also: Anthony J. Sassan, "Comparing Apples to Oranges: The Need for a New Media Classification (Case Note) *Cubby* v. *CompuServe Inc.* 776 F. Supp. 135 (S.D.N.Y. 1991)" (1992) 5 Software Law Journal 821.

217 http://www.eff.org/pub/Legal/Cases/Stratton_Oakmont_Porush_v_Prodigy /stratton-oakmont_porush_v_prodigy_et_al.decision

The situation of the Internet access provider must be approached in this manner. In order to define the liability assumed by such providers, we must ask what degree of control they have over the information found in the site. If we refer back to the criteria stated in *Cubby*, the level of control or supervision exercised by the electronic bulletin board operator or the site operator would be determining. Actually, it is difficult to exclude the liability of the site operator when it has deciding power over the posting of messages. This scale allows us to determine the level of liability which is incumbent on those responsible for sites open to the general public and sites reserved for closed groups. Their liability is closely related to the degree of control they exercise over the posting or making available of information.

4. Relations between Liability and Control Exercised over Information

In order to determine the liability of an actor which transmits the same information to many users at the same time, we must examine the relation such an actor has with the content of the message transmitted[218]. Moreover, the use of metaphors is one of the ways we can characterize the type of relationship an actor has, under given circumstances, with offensive information.

The goal and the scope of the rights and responsibilities of the various actors in electronic communications, including the access provider, do not depend so much on the official roles of such actors as they do on the degree of control such actors exercise, or are supposed to exercise, over the information and communications found in open networks or in the part of such networks over which they have some control. The assignment of liability to an entity presupposes the possibility of identifying the actors which control the information in the various spaces within such a virtual environment[219].

In effect, Perritt notes that the criterion of control over information plays a major role in the assignment of liability:

> In all three categories of tort liability (defamation, copyright infringement and invasion of privacy), the requisite fault cannot be proven without showing either that the actor and potential tort feasor exercised some actual control over content or that it was feasible for it to control content and that it could foresee the possibility of harm if it did not control content.[220]

Regarding this, Eric Schlachter writes:

> There is a sliding scale of control in relation to forced access. At one end of the scale are primary publishers, who have virtually unrestrained discretion over what they print or to whom they give access to disseminate information. Also on this end are owners of private property, who are similarly protected from mandatory or forced access. [...] At the other

---

[218] Jay R. McDaniel, *supra*, note 140 at 823.

[219] See Pierre Trudel, "The Protection of Rights and Values in Open-Network Management" in Ejan MacKaay, Daniel Poulin and Pierre Trudel, *The Electronic Superhighway: The Shape of Technology and Law to Come* (Amsterdam: Kluwer, 1996) at 159-193.

[220] Henry H. Perritt Jr., "Tort Liability, the First Amendment and Equal Access to Electronic Networks" (1992) 5 Harvard Journal of Law & Technology 65 at 110-111.

> end of the sliding scale from primary publishers are common carriers who by definition must be available to all comers and cannot refuse to provide service in a discriminatory fashion.[221]

This sliding scale concerns not only rights of access to electronic environments: it fully applies in the domain of liability. Schlacter points out that "Those entities with more editorial control generally also have greater exposure to tort liability for the statements or actions of others."[222] Thus, it is possible to determine the degree of liability from the degree of control a person effectively exercises over information in a given situation.

Editorial discretion, which is exercised mainly in traditional areas by an editor or broadcaster, guarantees freedom of editorial choices and that of the selection of information to be published[223].

It has been long recognized that governmental authorities do not have the power to interfere in the functioning of the traditional media. Note that *Reference re. the Laws of Alberta*[224] recognized the editor's power to determine the content of his or her publication, without any intervention from state authorities. The measures, or a municipal regulation on the distribution of pamphlets, made invalid in *Saumur*[225] were analyzed as allowing government authorities to use the content of documents to be distributed, instead of criteria other than content, as an argument to prohibit the distribution of information. For this reason, they were ruled invalid.

In *Gay Alliance Toward Equality* v. *Vancouver Sun*[226], a newspaper was accused of having contravened an anti-discriminatory provision of the *Human Rights Code* of British Columbia by refusing to publish a classified advertisement intended to promote the homosexual magazine *Gay*

---

[221] Eric Schlacter, *supra*, note 6 at 113 ff.

[222] *Ibid.*

[223] Susan D. Charkes, "Editorial Discretion of State Public Broadcasting Licensees" (1982) 82 Columbia L. Rev. 1161, 1172.

[224] [1938] S.C.R. 100.

[225] *Saumur* v. *Cité de Québec* (1953) 2 S.C.R. 299.

[226] [1979] 2 S.C.R. 435.

Alliance. Martland J., basing his argument on the *Miami Herald Publishing Co.* v. *Tornillo*[227] decision, reiterated that "[t]he law has recognized the freedom of press to propagate its views and ideas on any issue and to select the material which it publishes. As a corollary to that a newspaper also has the right to refuse to publish material which runs contrary to the views which it expresses."[228] He thus set aside an interpretation of an act which would have, in his eyes, the consequence of determining what a newspaper must publish. Editorial freedom supposes in-principle autonomy in decisions relating to the choice, treatment and distribution of information. In return for such freedom, there is responsibility: those who have editorial freedom must answer to third parties for the information distributed.[229]

Editorial liability does not take into account the intention to communicate a damaging message. What counts is the intention to communicate a message, the harmful nature of which should have been known by the editor[230]. Thus the editor is generally considered to be able to control the set of information which circulates in his or her enterprise[231], and such an editor answers for damages, whether the actionable statements come from an employee, an open letter to the editor, or advertising[232]. This power of control is what entails liability for the transmission of possibly illegal or harmful information[233]. The corollary is that those who play only a subordinate or minor role in

---

[227] 418 U.S. 241 (1974).

[228] *Gay Alliance Toward Equality* v. *Vancouver Sun* [1979] 2 S.C.R. 435, 455.

[229] Susan D. Charkes, *supra*, note 223 at 1161, 1172. This author thus demonstrates the intimate relation which exists in American law between the principle of editorial freedom and that of liability: "Editing - selecting of material to be communicated and deciding how to present it - is an activity protected by the First Amendment, although less so when the editor is a broadcaster. The guarantees of our system of free expression rest to a large extent on the assumption that autonomous editors will exercise judgment responsibly and, taken as a whole, will provide the public with necessary access to diverse views."

[230] Jay R. McDaniel, *supra*, note 140 at 817-818.

[231] Raymond E. Brown, *The Law of Defamation in Canada*, Second Edition (Toronto: Carswell, 1994) at 1219; David R. Johnson and Kevin A. Marks, *supra*, note 1 at 492; Robert Beall, "Notes: Developing a Coherent Approach to the Regulation of Computer Bulletin Boards" (1987) 7 Computer/Law Journal, 499 at 505.

[232] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 492.

[233] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 492.

the process leading up to publication incur liability only if their negligence is clearly demonstrated[234].

The exercise of editorial discretion and its consequences on the level of assignment of liability were discussed in *Cubby*. An electronic message distributed on CompuServe contained unflattering remarks about a rival (Cubby). The court ruled that "Compuserve has *no more control* over such a publication than does a library, book store or newsstand"[235]: the information, established by an independent third party, was entered directly into the system to provide immediate access to users. For this reason, and because the extremely elevated number of messages in the system made it impossible to examine them[236], the court concluded that CompuServe could not know, or have a reason to know, of the harmful nature of the messages. CompuServe was thus not liable for them.

According to Eric Schlacter, it is important to interpret the law in a manner which takes into account new information technologies. To this end, a relation between the degree of editorial control and liability can be recognized.

An access provider, a system operator or any other actor can, depending on innumerable possible circumstances, have different degrees of control over information[237]. Depending on the degree of control effectively exercised, the liability will be more or less great.

Effective Physical Control and Information Longevity

Effective physical control is exercised by a person who, knowing that he or she is participating in the broadcast of a potentially damaging message, has the possibility of withdrawing such a message and ending its circulation not by exercising editorial control over the content, but by withdrawing the material support of the content or the entire "work"[238]. That such a factor should be considered when liability is to be assigned is simply common sense: [TRANSLATION] "an

---

234 Raymond E. Brown, *supra*, note 231 at 1220; *Weldon* v. *"The Times" Book Co.* (1911) 28 T.L.R. 143 (C.A.).

235 *Cubby Inc.* v. *CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991) at 140.

236 *Cubby Inc.* v. *CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991) at 140.

237 Eric Sclacter, "Electronic Networks and Computer Bulletin Boards: Developing a Legal Regime to Fit the Technology", http://www.seamless.com/eric/eric-1.html.

238 Here "work" refers to the complete set of information considered as a whole.

individual cannot be held responsible for an unforeseeable and inevitable act over which he or she had no control."[239] In contrast, the courts demonstrate a natural tendency to assign liability to those who were reasonably capable of acting to prevent the damage.

Many examples taken from traditional communications contexts (press, radio, television, printed publication) show that the possibility of exercising effective control over the medium used to circulate information can be one of the factors in assigning liability if the actor in question did not take the precautions available to remedy the damage after its initial publication or broadcast.

One such example can be found in the regime applied to secondary publishers. Secondary publishers are persons who participate in the publication process, but in a limited manner. A secondary publisher is liable if it knows or had reason to know of the defamatory nature of the message transmitted[240]. Likewise, jurisprudence considers that a printer cannot be held responsible for the defamatory content of works written by its clients since it does not have the duty to revise the content of the works it prints and it is presumed to not know their content[241].

A similar regime is applied to the re-broadcaster, in other words someone who circulates or sells material *published by others*[242]. The status which best illustrates the possibility of performing this sort of control is that of an information distributor. A librarian, like a bookseller, distributes

---

[239] Nicole Vallières and Florian Sauvageau, *supra*, note 105 at 25-26.

[240] *Lerman* v. *Chuckleberry Pub. Inc.*, 521 F. Supp. 228, 235 (S.D.N.Y. 1981); David J. Loundy, *supra*, note 178.

[241] *Maynard* v. *Port Publications Inc.*, 297 N.W.2d 500 (Wis 1980).

[242] Eric C. Jensen, *supra*, note 183; Joseph P. Thornton, Gary G. Gerlach and Richard L. Gibson, *supra*, note 161 at 179.

information. In other words, he or she delivers or circulates information - while a re-broadcaster repeats it[243]. Normally, a distributor does not control the content of the information it transmits and thus has no liability if it is damaging[244]. It would in effect be unthinkable for each distributor (newspaper vendor, book store, library) to have the duty to verify the content of each publication it distributes in order to ensure that it contains no harmful information[245].

However, since the distributor has physical control over the material published, it has the duty to make reasonable inquiries into the accuracy of statements when it is informed that they are potentially harmful[246]. If such inquiries lead it to the conclusion that the statements in question could indeed by harmful, it has the obligation to withdraw them from circulation. While the distributor does not have an editor's control over the content of a book, it always retains the ability to remove a book from the book store shelves. If the distributor fails to do so, it may be held liable for the damages caused by the statements[247].

In the *Cubby* decision, the judge applied the standard of distributor to CompuServe: it was held liable if it "knew or should have known":

> the inconsistent application of a lower standard of liability to an electronic distributor such as CompuServe, than that which is applied to a public library, book store or newsstand, would impose an undue burden on the free flow of information.[248]

---

[243] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493.

[244] Trotter Hardy, *supra*, note 187 at 1003; David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493.

[245] *Balabanoff* v. *Fossani*, 81 N.Y.S.2d 732, 733 (Sup. Ct. 1948).

[246] Henry H. Perritt Jr., *supra*, note 220 at 106.

[247] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493; David J. Loundy, *supra*, note 178.

[248] *Cubby Inc.* v. *CompuServe Inc.*, 776 F.Supp. 135 (S.D.N.Y. 1991) at 140.

Because of the speed of information transmission, and the great number of transmissions, CompuServe could exercise no physical control except at the level of the complete work. While CompuServe has the choice whether to circulate a work, once a work is in its system, it can exercise no editorial control over it[249]. Since it was not established whether CompuServe "knew or should have known" that the publication in question contained harmful information, no liability was assigned to it.

The longevity of the information, like the effective control of it, has a direct influence on the possibility of exercising control. In effect, liability will not be evaluated in the same way when the information is stable and when it continuously varies. Variable information changes regularly, sometimes every few seconds (for example, financial data), and thus it is not only virtually impossible to revise its content as it is transmitted for use, or to provide remedies if such information is false or inaccurate[250], there is greater difficulty in stopping its circulation before damage is suffered.

In contrast, information which remains relatively stable is much more amenable to control. Moreover, the user is much more justified in relying on such information because its stability implies that the provider has taken the trouble to confirm its accuracy[251].

In the telematic domain, a relation is identified between control and prior fixing of information:

> [TRANSLATION] However, it should be noted that these delicts [defamation] presuppose that the message has already been fixed. The idea is that the publisher must control what it disseminates, but that it be able to do so. . . . This point is extremely important in the context of our discussion when an entire portion of the messages available on line, and therefore the content thereof, is not seen by the service provider. Liability therefore arises in this case only where the message has been stored (before being made available to the public). The time factor is irrelevant: it suffices that the service provider was in a position to exercise the control it is required by law to exercise.[252]

---

[249] "While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a publication, it will have little or no editorial control over that publication's contents. This is especially so when CompuServe carried the publication as part of a forum that is managed by a company unrelated to CompuServe": *Cubby Inc.* v. *CompuServe Inc.*, 776 /f.Supp. 135 (S.D.N.Y. 1991) at 140.

[250] Joseph J. Tiano Jr., "The Liability of Computerized Information Providers: A Look Back and A Proposed Analysis for the Future" (1995) 56 University of Pittsburg Law Review 655, 684.

[251] *Ibid*., at 685.

[252] Michel Vivant, Ed., *Lamy droit de l'informatique* (Paris: Lamy S.A., 1996) at 1206, No. 1893.

Perritt nonetheless emphasizes that the possibility of exercising such physical control does not result uniquely from technological factors:

> The victim would prefer a rule that would allow a defendant to avoid tort liability only in situations in which content control is technologically infeasible. Infeasibility, however, is a concept with an economic dimension. Determining what is feasible requires balancing of risks and benefits.[253]

This is why we necessarily find ourselves back at the issue of knowledge of the harmful nature of the information.

---

[253] Henry H. Perritt Jr., *supra*, note 220 at 110-111.

5. Relations Between Liability and Knowledge of Information

Knowledge of the harmful nature of a piece of information is strictly linked to many factors in the assignment of liability. This is why they are dealt with, in certain instances, concurrently. The knowledge issue does not usually come up in editorial contexts in which knowledge of the harmful nature of the information is accompanied by a presumption of knowledge inherent to the exercise of editorial discretion: faith in editorial decisions in no way tempers the entailed liability[254]. To publish is to communicate information to third parties knowing that such information will be read, seen or heard. As a result of the exercise of editorial freedom, publication supposes first-hand knowledge of the existence of the information transmitted[255].

While editorial discretion entails a presumption of knowledge of the harmful nature of the information transmitted, in the absence of editorial power, knowledge must be established for liability to be assigned. Knowledge can be assigned under many circumstances:

> Knowledge, or the imputation of knowledge, can be established if the intermediary exercized content control over the messages on the network (ex.: moderator of a bulletin board conference who screens messages before posting them) or if special circumstances were present, such as the fact that the operator knew of the user's repeated transmission of defamatory messages and had knowledge that a recent message may be defamatory. This special circumstance may arise even if an intermediary that otherwise does not exercise content control receives complaints about an originator of messages.[256]

Yet how is it possible to impose a duty to prevent damages following the broadcast of information the harmful or illegal nature of which is likely to be determined only by a court decision? The same question arises following the emphasis of the harmful nature of a piece of information: what credibility must be granted to external sources of knowledge? What re-evaluation of this information must then take place?

---

[254] Jean-Louis Baudouin, "La responsabilité causée par les moyens d'information de masse", (1973) R.J.T. 201, 203.

[255] Loftus E. Becker Jr., *supra*, note 162 at 217.

[256] Henry H. Perritt Jr., *supra*, note 220 at 107.

These questions were asked in *Religious Technology Center* v. *Netcom Online Communication Services Inc.*[257] in an intellectual property context, which is however applicable to more global contexts. An anonymous user made available, through the intermediary of a discussion group, material copyrighted by the Church of Scientology. As soon as the latter was made aware of the infringement, it asked the system operator to remove the material. The system operator refused to act until it had obtained supplementary evidence. The judge ruled that Netcom was made liable through its failure to act, which amounted to substantial participation in the illegal distribution of material.

Though it does allow us to focus on certain specific issues[258], this judgment does not provide any precise guidelines. In this case in particular, evidence revealed that Netcom had done nothing to stop the distribution of *potentially* illegal material and that it had even refused to look at the material in question. Still, what weight must a notification have to create a duty for a system operator, or any other intermediary which could prevent damage by stopping the circulation of the material, when the policy of the latter is to exercise no editorial control over the content it helps to circulate?[259]

While the safest solution would be to take action on each notification, such a practice would be incompatible with the freedom and openness to debate which exists on the Internet[260]. Moreover, it is unrealistic from the point of view of the access provider. The volume of information is so great that many such providers could receive numerous notifications of which the validity would be difficult to determine.

Another possible solution would be to protect the intermediaries from any liability until a legal decision has been made on the harmful, illegal or infringing nature of certain information, which could be removed from distribution. However Perritt demonstrates the weakness of such an approach, in particular in the case of broadcast of content infringing on intellectual property rights:

---

[257] 907 F. Supp. 1361 (N.D. Cal. 1995).

[258] "Does the notice of violation identify which materials are at issue? Does it provide specific evidence of copyright ownership or just a vague claim?": "The Scientology Lawsuits and Lawyer Letters: The Problem Faced by On-line Services Who Get Notice of Users' Alleged Violations", Legal Bytes, Spring 1996, Vol. 4, No. 1, http://www.gdf.com/1b4-1.htm.

[259] "The Scientology Lawsuits and Lawyer Letters: The Problem Faced by On-line Services Who Get Notice of Users' Alleged Violations", Legal Bytes, Spring 1996, Vol. 4, No. 1, http://www.gdf.com/1b4-1.htm.

[260] *Ibid.*

> ...that approach would not adequately protect the interests of copyright holders. It takes a long time to get a judgment on the merits in most jurisdictions and continued availability of infringing materials while the litigation process proceeds could result in substantial irreparable harm to the copyright holders.[261]

The notion of knowledge will also be shaped by the damage likely to be caused. For example, defamation results by definition in a negative perception held by third parties, a criterion based on the perceptions of an ordinary person[262]. As soon as it is presumed that the exercise of editorial freedom leads to contact between the editor and all content published, it is taken for granted that the editor, as a reasonable person, knew that the statements with which he or she had been in contact could harm the reputation of the person they targeted, but that he or she nonetheless published them.

In the case of certain types of information, it is often impossible for intermediaries, which were in no way responsible for the establishment of such information, to know if it is inaccurate and thus capable of causing harm. In such cases, presumed knowledge will thus be necessary for the assignment of liability:

> It may well be argued that the producer will be liable if he publishes or fails to correct inaccurate data after he discovers it is unreliable, at least if he is aware of their potentially damaging nature. [...] On the other hand, liability may be limited because the defendant knew, or at least should have been aware, that the data were not reliable.[263]

The question is, however, whether a regime of presumed knowledge will not have the practical consequence of transforming network operators into editors.

---

[261] Henry H. Perritt Jr., "Computer Crimes and Torts in the Global Information Infrastructure: Intermediaries and Jurisdiction", (12 October 1995), http://www.law.vill.edu/chron/articles/oslo/oslo12.htm.

[262] N. Vallières, *supra*, note 39 at 20.

[263] Jaap H. Spoor, "Database Liability: Some General Remarks", (April 1989) 3 International Computer Law Adviser 4, 6.

6. Relations between Liability and the Role Assumed in Information Dissemination

There are certain links between the role assumed in the dissemination of information and the liability following from that role. These links are entailed by principles applicable to the liability of intermediaries.

The new information technologies have stimulated analyses oriented toward a reformulation of the rules under which intermediaries in the information chain are held responsible for harmful information created by someone else[264]. What are the foundations of the attribution of liability to intermediaries in the information chain?

While civil liability law in common law is built around duties of diligence[265], civil law approaches liability from the point of view of the prejudice suffered, and not the obligation which may have preceded it: the extent of liability is greater because any one who causes a loss or prejudice following unreasonable conduct is liable to provide compensation for the damages suffered[266].

> [TRANSLATION] The essentially compensatory function of liability is based, *inter alia*, on an idea, which had already emerged in the second half of the 19th century and subsequently became increasingly influential, that damage should not be compensated for only when it was preventable; on the contrary, it should be possible to obtain compensation through liability even where there was no prevention.[267]

In civil law, the liability of intermediaries is due to the fact that [TRANSLATION] "It must in fact be understood . . . that in law, the question is less to determine who is in the wrong, which has the

---

[264] Henry H. Perritt Jr., *supra*, note 261.

[265] "First one has to ask whether as between the alleged wrong-doer and the person who has suffered damage there is a sufficient relationship of proximity or neighbourhood such that, in the reasonable contemplation of the former, carelessness on his part may be likely to cause damage to the latter in which case a prima facie duty of care arises": *Anns* v. *London Borough of Merton*, [1977] 2 All. E.R. 492 (H.L.).

[266] J. Huet, *supra*, note 124 at 107.

[267] Christian Larroumet, "Reflexions sur la responsabilité civile: évolution et problèmes actuels en droit comparé", (Montréal: University of McGill, Institut de droit comparé, 1983) at 16.

connotation of a value judgment, than to determine who is liable in the sense of a person who must answer for a specific fact."[268] For some, liability rests essentially on the notion of risk:

> [TRANSLATION] The basis for the right to compensation is not a fault that caused damage but the very fact that damage occurred in such circumstances that it seems unfair to let the victim bear its weight. Thus, it is the concept of the risk that caused the damage that seems to be the source of liability.[269]

A recent Québec Court of Appeal decision, however, rejected the point of view that the liability of media and journalists rests on a concept of risk linked to their activities. Instead, their liability would be like professional liability, which refers to the criterion of a reasonable person working in such a sector of information[270].

Intermediary responsibility can result from the jurisdictional or practical impossibility of holding the true author of the harmful message. This concern is particularly relevant in the context of electronic communications:

> Tort liability imposed on an intermediary is a kind of default rule or safety net, recognizing that there may be instances in which the person with fault - the originator of the harmful message or file - would be unavailable, beyond the jurisdiction of any tribunal available to the victim, or judgment proof. Thus, the policy question for intermediary liability is whether the victim should bear the loss when the originator cannot be found, or conversely when the intermediary should bear the loss.[271]

The question of intermediary liability is not entirely separate from issues of national jurisdiction. Since the new information-highway communications technologies allow a person situated at one point on the globe to inflict prejudice on another elsewhere by simply sending an electronic message, the difficulties in identifying the actor and obtaining compensation from him or her naturally moves attention from the victim of the damages to the intermediaries which are likely to

---

[268] Michel Vivant et al., *Lamy droit de l'informatique: informatique, télématique et réseaux* (Paris: Institut de France, Lamy S.A., 1996) at 460, No. 719.

[269] Patrice Jourdain, *Les principes de la responsabilité civile*, Second Edition (Paris: Dalloz, 1994) at 28.

[270] *Société radio-Canada* v. *Radio Sept-Iles Inc.*, (1994) R.J.Q. 1811, 1819-1820, Le Bel, J.

[271] Henry H. Perritt, *supra*, note 261.

be more easily identified, subject to the jurisdiction of traditional legal institutions, and financially able to provide compensation for the prejudice.[272] In effect,

> [TRANSLATION] Still other bases are suggested to justify liability without fault in certain cases: the first is the guarantee of solvency that enables victims to designate respondents who are ordinarily more solvent than those who actually caused the damage.[273]

Another foundation of intermediary liability is the role as a contributor to and amplifier of the damage. Intermediaries would be subject to greater liability than that of the creators of the harmful communication because the intermediary's channel increases both the possibility of a tort and the severity of such a tort[274]. However, we must not underestimate the consequences of the imposition of an excessively strict standard of liability regarding intermediaries in the information chain.

---

[272] *Ibid.*

[273] Patrice Jourdain, *supra*, note 269 at 30.

[274] Henry H. Perritt Jr., *supra*, note 261.

7. Preventive Techniques for Distributing Civil Liability among Participants in Internet Communications

Self-regulation refers to standards developed voluntarily and accepted by those engaged in an activity[275]. The primary aspect of self-regulatory rules is that they are voluntary, in other words they are not obligatory as is a legal regulation passed by the State. When a subject is governed by self-regulation, that subject has generally consented to be so. Such regulation is essentially contractual. Most often, adherence to self-regulatory standards is adopted because it presents more advantages than disadvantages.

Private associations have, in many areas of activity and with varying intensity, developed voluntary ethical principles and technical standards. In service domains such as sales[276], advertising[277], banking[278], property values[279], accounting[280], media[281], this is mainly the form

---

[275] Pierre Trudel, "Les effets juridiques de l'autoréglementation", 91989) 19 Revue de droit de l'Université de Sherbrooke, at 251.

[276] Kenneth Cohen and Ian Rocher, *Self-regulation by Industry: An In-Depth Study of the Better Business Bureau* (Toronto: Osgoode Hall Law School, 1974).

[277] James P. Neelankavil and Albert B. Stridsberg, *Advertising Self-Regulation: A Global Perspective* (New York: Hastings House, 1980); Dominique Forget, *Le fonctionnement des organismes d'autoréglementation de la publicité au Canada*, Master's thesis in Communications, Université de Montréal, 1989; Maurice Watier, *La publicité* (Montréal: Éditions Paulines & Médiapaul, 1983) at 95 ff.; Bernard Motulsky, *La publicité et ses normes* (Québec: P.U.L., 1980); Daniel Jay Baum, "Self Regulation and Antitrust: Suppression of Deceptive Advertising by the Publishing Media" (1961) 12 Syracuse L.R. at 289.

[278] David G. Oedel, "Private Interbank Discipline" (1993) 16 Harvard Journal of Law & Public Policy at 327-409; Jean Pardon, "Quelques normes propres au secteur bancaire" in Commission droit et vie des affaires, *Le droit des normes professionnelles et techniques*, Seminar organized at Spa-Balmoral, November 16-17, 1983 (Brussels: Bruylant, 1985) at 1-46.

[279] See David L. Ratner, "Self-Regulatory organizations" [1981] 19 Osgoode Hall L. J. at 368; Alan C. Page, "Self-Regulation: The Constitutional Dimension" [1986] 49 Mod. L. Rev. at 141.

[280] Canadian Institute of Chartered Accountants, *CICA Manual* (Toronto: 1968).

[281] Francis Coleman, "All in the Best Possible Taste: The Broadcasting Standards Council 1989-1992" (1994) Public Law 488-515; Daniel L. Brenner, "The Limits of Broadcast Self-Regulation Under the First Amendment" [1975] 27 Stanford L. R. 1527; Harvey C. Jassem, "An examination of Self-Regulation of Broadcasting" [1983] 5

voluntary regulation has taken. Such ethical codes aim to promote precepts recognizing "honest practices" or practices in conformity with what is considered proper in the domain of professional or commercial activity in question[282].

Voluntary associations have sometimes attempted, with varying success, to establish ethical standards. Such standards of conduct are sometimes set out in codes of ethics adopted by the administrations of the associations, or result from the set of decisions made by organisations which have set themselves the task of enforcing respect for the code of ethics and related practices within an industry or professional group. Many self-regulatory rules take the form of recommendations. They are issued by specialized organisations and are most often imposed due to the expertise possessed by such organisations[283].

The practice in electronic environments, especially in the Internet, reveals the principal models of self-regulation prevailing there. Thus, those controlling a site in the network have the possibility of adopting policies regarding access to the site, acceptable behaviour, and prohibited acts. Most university institutions have adopted policies or rules defining the rights and obligations of those using the computer resources of the institution. As is explained in a document from the American Research Council,

> Many universities govern their electronic networks through campus policies that are substantially the same as the policies governing other pieces of university infrastructure. Freedom of speech [...] tends to be an overriding value on these networks, based on the principles of academic freedom. But incidents challenging this freedom arise frequently. Jeffrey I. Schiller, network manager at the Massachusetts Institute of Technology, for example, notes that at least once a month someone asserts harassment as the result of someone else's electronic free speech. The values that govern behavior may be blurred further by campus connections through the Internet and to other institutions or

---

Communications and the Law 31. The opportunity to use self-regulation to replace state regulation was subject to heated debate in Autralia. See Michael Blakeney, "Leaving the Field - Government Regulatory Agencies and Media Self-Regulation" [1986] 9 U.N.S.W. L. J. 53-65; Australian Broadcasting Tribunal, *Self-Regulation for Broadcasters, A Report on the Public Inquiry into the Concept of Self-Regulation for Australian Broadcasters*, July 1977. Regarding Canada, see Pierre Trudel, *Le rôle des standards déontologiques dans le cadre normatif de l'information*, Report presented at the Congrès de la Fédération professionnelle des journalistes du Québec, Québec, December 5, 1986.

[282] D. J. Lecraw, *Voluntary Standards as a Regulatory Device*, Ottawa, Economic Council of Canada, Regulation Mandate, Research Paper No. 23, 1981 at 30 ff.

[283] See: "Private Codes for Corporate Conduct: Should the Fox Guard the Henhouse?" [1993] 24 Interamerican Law Review, 399-433; Olivier Hance, "L'évolution de l'autoréglementation dans les réseaux informatiques: éléments pour la construction d'un modèle théorique" (August 1994) Journal de réflexion de l'informatique; S.F.Stager, "Computer Ethics Violations: More Questions than Answers" Educom Review, July-August 1992, 27-30.

> organizations that may have different values. "And the only thing that has made the situation tenable has been the fact that most of the policies have significant amounts of overlap and nobody is enforcing them", Schiller said. "Only the most outrageous behavior will ever raise an eyebrow [...]".
>
> A different balance of values is found in the world of commercial network service providers. Commercial providers are highly motivated to provide a range of network services that appeal to large audiences and generally try to suppress message traffic found offensive by significant segments of these audiences. For example, a commercial provider will often explicitly prohibit overtly sexual real-time chats on its network.[284]

Such policies, which are sometimes made explicit in official documents and in membership contracts signed by members and clients, state the guidelines on behaviour related to issues such as: the private nature of electronic mail, the conditions on the use of software available on the network, the obligation to use one's real name, the right to engage in commercial advertising, the right to use network resources for personal ends, and liability for the behaviour of members and clients.

There are already numerous forms of self-regulation in electronic environments. Centralized commercial information services have established detailed policies and apply complaint answering and dispute resolution procedures. As for regulation of the Internet, which obeys no central authority, it falls under informal agreements between all users, as well as the more formal agreements of server owners established all over the planet. Thus, the rules of the game are first formulated in contracts between users and access providers: these are known as *acceptable use policies*. Such standards, which are generally the same from one network to another, list a series of prohibited behaviours.

At another level, the standards developed in the framework of electronic environments reflect the habits and practices developed by the users of such electronic environments. Moreover, a neologism, "Netiquette", describes the principles of good conduct generally recognized by Internet users. Those who employ Usenet also have their own arrangements regarding conduct to be followed and, if applicable, the remedies and sanctions to be applied. Curiously, the existence of a large number of networks and virtual communities, each obeying its own rules, could lead either to a divided or to a homogenous legal regime[285].

---

[284] Dorothy E. Denning and Herbert S. Lin (Ed.), *Rights and Responsibilities of Participants in Networked Communities* (Washington D.C.: National Press Academy, 1994) at 20-21. Posted on the site http://www.nap.edu/readingroom/books/rights/.

[285] David Post, "Anarchy, State and the Internet: An Essay on Law-Making in Cyberspace" (1995) J. Online L. s. 3, posted on the site: http://warthog.cc.wm.edu/law/publications/jol/post.html, par. 27: "Saying that cyberspace may consist of a large number of individual networks, each with its own rules (about, e.g., the propriety of obscene text and the definition of "obscenity") does not tell us whether or not the law of cyberspace will in the aggregate consist of a diverse

Since a certain number of "universal" standards could be identified, Robert Dunne proposed the codification of the rules of "frontier justice" presently employed. According to him, such a code could resemble the following:

> - A model code of network conduct would specify offenses, such as unauthorized access and attempted unauthorized access, and the range of their penalties;
>
> - Internet host sites and other providers of Internet access would be expected to endorse this code and enforce it;
>
> - Participating sites and providers would limit access to their resources by other sites and providers to those who had endorsed the code, or at least severely restrict access by those who had not;
>
> - All Internet users at participating sites or obtaining access through participating providers would be required to sign an agreement accepting the terms of the code of conduct;
>
> - Users wishing to use an alias for Internet identification would be required to register that alias with the local site or provider;
>
> - Enforcement would be local by the various host sites and network access providers, as it is already for the most obviously agreed upon offenses.[286]

David Johnson anticipates that self-regulation will develop from rules applicable between network operators and their users, and then spread to all networks in a more or less transparent manner. According to him, a "A `Cyberspace Law Institute' might provide the mechanism for such lawmaking as follows":

> (1) Any new proposed rule would be published in an easily accessible place and distributed by mail to a list of sysops and others interested in reviewing such proposals;

---

set of such rules or will converge on a single, or a small number, of such rules. To analyze that question we need to examine one additional feature of the competition among controllers."

[286] Robert Dunne, "Deterring Unauthorized Access to Computers: Controlling Behaviour in Cyberspace Through a Contract Law Paradigm" (1994) 35 Jurimetrics J. 1, 13, and posted on the site http://www.cs.yale.edu/pub/dunne/jurimetrics/jurimetrics.html. The author recognizes that it may be difficult to reach a consensus regarding a code of conduct which participants would endorse. In this respect, he indicates that a specific domain, such as that of teaching institutions, could promote the adherence of other groups, in particular through the threat of restrictions on access.

> (2) All comments and debate would be collected in that same electronic location and distributed to interested parties;
>
> (3) Sysops prepared to accept and enforce the rule would register their agreement at the central location;
>
> (4) Vigourous opposition to particular rules, coupled with an indication of unwillingness to connect to systems that adopt the proposed rule, could also be registered;
>
> (5) After a suitable interval, the sysops who agree upon the rule would proceed to implement and enforce it. Presumably, one first rule would be that sysops will not connect with other systems that do not enforce the rules that those systems have agreed upon. Another first principle might address the amount of "due process" to be given a user, perhaps including appeal to a decision maker other than the local sysop, before invocation of the ultimate sanction.[287]

To a large degree, the proposition that the legal regime of electronic environments should rest on law between parties, contracts, tends to illustrate the strong tendency toward self-regulation which can be seen at the present time. A number of authors predict, moreover, that the legal regime which will govern electronic spaces will be very similar to the *lex mercatoria* of the Middle Ages. In other words, it will be based on a set of business customs developed and accepted by all, and applied separately from traditional legal institutions. The contractual practices engaged in by the participants will likely be called upon to play a major role in the development of this yet-to-be-defined legal regime. The same could be said of the doctrine and jurisprudence, and of the recommendations and model codes adopted by specialized international institutions.

Some propose the development of a code of conduct to which Internet service providers could adhere. For example, regarding the circulation of hate propaganda, Rabbi Abraham Cooper of the Simon Wiesenthal Centre proposes that if a user engages in the distribution of information which is judged illicit under the code of conduct, the providers in question could cut off his or her Internet access and force that user to find another entry:

> It's a paid relationship: you pay your nickel and you get your access. [...] If an individual or a human-rights group complains about a site that "crosses the line" the Internet provider should say, "Here's your nickel, go play somewhere else."[288]

---

[287] David Johnson, "Lawmaking and Law Enforcement in Cyberspace", posted on the site http://www.cli.org/DRJ/make.html.

[288] A. Riga, "Online Against Hate" (Saturday, March 16, 1996) *The Gazette* B-2.

Thus the Canadian Association of Internet Providers recently adopted a Code of Conduct in which it is stated that: "CAIP members will not knowingly host illegal content. CAIP members will share information about illegal content for this purpose."[289] The Code also recognizes that "Sharing information about material that has been evaluated as illegal will facilitate some preventative action."[290]

Yet the limits of such a mechanism must be recognized. A client may always deal with another provider. The Code admits this in the following terms:

> The Internet is designed to route around blockages, therefore, despite any effort or step taken by a CAIP member, users who wish to obtain or publish illegal content may be able to obtain it from sources or sites outside the control of CAIP members.[291]

Self-regulatory initiatives such as these do not eliminate offensive content any more than they give access providers immunity from all civil liability. However, they can be useful tools for making the best-placed participants in Internet communications more responsible in reacting to problem communications. Thus, an access provider adhering to a code such as that of the CAIP will indicate the guidelines it intends to follow. Such rules could contribute to demonstrating that the access provider has taken the necessary precautions to prevent actionable information from being carried on its network. In many cases, this factor, combined with that entailed by the fact that the access provider cannot know about everything being carried on the Internet, certainly contributes to defining the scope of its liability.

Conclusion

We have seen that several situations in which the liability of the Internet access provider can become an issue are governed by the principles of civil liability. The principles of civil liability are stated in the law of each province since it is an area which falls under provincial jurisdiction in virtue of the Constitution.

In nine provinces this area is governed by Common Law, while in Québec it is ruled by the Civil Law principles of the French tradition. While the Civil Law system is based on a set of principles recorded in a code which is used to decide specific cases, the Common Law approach is to

---

[289] Canadian Association of Internet Providers (CAIP) "Code of Conduct", http://www.caip.ca/caipcodf.htm, s. 5.

[290] Canadian Association of Internet Providers (CAIP) "Code of Conduct", http://www.caip.ca/caipcodf.htm, s. 5.2.

[291] Canadian Association of Internet Providers (CAIP) "Code of Conduct", http://www.caip.ca/caipcodf.htm, s. 5.1.

examine decisions handed down in earlier cases in order to induce the principles which should be applied in the situation to be resolved. This explains the great importance of court decisions in the latter system. In spite of these differences in approach, both systems usually lead to equivalent decisions.

In general, civil liability law concerns situations in which harm is suffered by a person due to an activity. The law then determines the situations in which there is liability, who assumes such liability and the way in which the prejudice will be compensated. The principal situations which can generate damages and civil responsibility are those which include justiciable actions performed by those involved which cause:

- harm to reputation (defamation)
- invasion of privacy
- violation of secrecy
- unfair competition

In each of these situations, liability is not automatic and is not necessarily assigned to the access provider. Liability does not depend on what one is, but rather on what one does or does not do when transmitting information. It is generally after careful examination of the specific facts of each case that it can be determined whether there was justiciable, clumsy or negligent action taken by one of the participants in the production and transmission of a message which proved to be harmful. This is the context in which the access provider's liability can come into question.

The principles of civil responsibility as they are understood in Common Law and in Québec Civil Law establish a strict relation between the degree of effective control over information and the liability of the various participants in the communications. The nature and degree of the liability of Internet access providers clearly follows from the degree of control they exercise or are supposed to exercise over harmful information. This entails that when the specific circumstances of a case of broadcast of actionable information reveal that the access provider had some control over the incriminated information, that provider will be assigned a share of the liability. In corollary, an access provider which is warned of the existence of problem content risks being found liable if it fails to intervene.

However, in the present state of the law, it remains difficult to distinguish the circumstances in which an access provider should act to prevent prejudice from those situations which do not present a sufficiently clear case to justify an intervention which often could result in severe censorship. Without having access to the viewpoints of all those involved, it is indeed very difficult to determine whether a specific content is actionable. The access provider thus finds itself in the uncomfortable position of being criticized at some point for having permitted a content harming a person to circulate, when it is really very poorly placed to intervene in order to

suppress a content of which the harmful nature is often far from obvious. Moreover, the principle of freedom of expression as it is understood in democratic societies concords poorly with practices in which access providers would pass judgment on the potentially actionable or harmful nature of information passing through their facilities.

The present state of civil liability law calls for access providers to adopt preventive policies in order to manage their responsibility in the manner which is most compatible with the Internet and so as to minimize, for themselves as for others, the harm which could be caused by actionable information on the Internet.

In such a spirit, the policies and self-regulatory mechanisms which are regularly brought to the attention of users, such as the Canadian Association of Internet Providers' Code of Conduct, are preventive measures. They help to distribute responsibility among the actors and testify to a real concern of access providers that clearly illegal or harmful content should not be tolerated, while they do not lead such actors to exercise control over content circulating in an environment which they do not control *a priori* and which they do not claim to control.

[Cat. N.: C2-312/1997E ISBN: 0-662-25489-9]

CONTENT-RELATED LIABILITY FOR COPYRIGHT INFRINGEMENT ON THE INTERNET

Mark S. Hayes[1]

1. INTRODUCTION

The Internet has exploded into the consciousness and homes of Canadians like nothing since the advent of television more than 50 years ago. Every day sees newspaper and magazine stories on the growth of the Internet, its potential commercial impact or its imminent demise. An entire genre of magazines dealing solely with the Internet has appeared like magic on our bookstore shelves.

Copyright has been a legal concept which has been fundamental to the development, growth and exploitation of the artistic and entertainment products which enrich our lives. In addition, with the development of computers and the software to operate them, copyright law has assumed an important role in protecting the economic rights of the creators of software programs. Intellectual property and the protection offered to its creators by copyright will continue to grow in importance.

The rapid growth of the Internet has leapfrogged legal developments and created uncertainty about the nature of rights in an environment which is wholly new.[2] While great opportunities await those entrepreneurs which can seize the day and build the Internet of tomorrow, the potential costs involved are staggering. If there is uncertainty about the extent of the liability which may be incurred, necessary investments may be delayed or withheld, to the detriment of all. While it is never possible to define exactly what risks are inherent in any new venture, particularly one as revolutionary and technological as the Internet, a reasoned analysis of the likely risks can be of great assistance to the Internet community and the public at large.

This uncertainty is of particular importance to Internet intermediaries, including Internet Service Providers (ISPs), on-line services, bulletin board service (BBS) operators and telecommunications suppliers. If their liability in operating the Internet turns out to be such that prudent and reasonable entrepreneurs are dissuaded from making investments in the equipment and systems required to permit the Internet to grow and expand, the potential of the "Information Highway" will not be realized.[3]

---

1 Partner, Fasken Campbell Godfrey / Fasken Martineau, Toronto, Ontario; http://www.fasken.com.

2 For an interesting discussion of the basis for copyright law and the limits 1of its application the Internet environment, see Elkin-Koren, "Copyright Law and Social Dialogue on the Information Superhighway", 13 Cardozo Arts and Entertainment L.J. 346 (1995).

3 In their brief to this study (and elsewhere) the Canadian Association of Internet Service Providers (CAIP) referred to this uncertainty as an "impending liability crisis".

On the other side of the copyright equation, creators and owners of copyright works need to know the extent to which their works will be protected on the Internet, either by effective legal mechanisms to combat infringement or by adequate remuneration for use of their works on the Internet. There is much uncertainty within the creative community concerning the safety of the Information Highway, and many creators are withholding works from the Internet and other electronic forms of dissemination until they have a better idea of what the exploitation of their works is worth in these media and are assured that the legal and economic framework which protects their creations is adequate.[4]

Without new and varied content provided by creators, the Internet is ultimately a useless accumulation of technology. "Consumers will not demand ... an information superhighway if it is merely an alternative way of sending messages, playing games or watching television, but only if it is "application rich" - replete with creative content and services of all kinds that are practical, affordable and valuable to the user."[5]

This paper is intended to perform a relatively narrow function in the cacophony of discussion and debate about the Internet and the protection of copyrighted works. It will attempt to state, with as much certainty as is possible in the circumstances, the legal framework which applies to liability for copyright infringement in Canada as a result of the content contained in transmissions over the Internet. The study will examine the law under the current Canadian *Copyright Act*, although reference is made to certain of the amendments proposed in Bill C-32. No attempt will be made, except in passing, to suggest reforms of the legal framework, although some of the most obvious uncertainties in the current law are discussed.[6]

---

4 Estimates of the amount of copyright material stolen worldwide by infringers range into the tens of billions of dollars. "It is quite possible, for example, for a computer program that cost millions of dollars to develop to be released on Monday, improperly obtained on Tuesday, uploaded to the Internet on Wednesday, shareware by Thursday, and worthless freeware on Friday.": Cook, "Deputizing the ISPs", available at http://www.ipmag.com/acook.html. The only possible error in this description is that the time frame described is too extended; things can happen much faster on the Internet.

The theory that creators will not produce works if their copyright is not protected has historically been the subject of some controversy: see the classic debate in Breyer, "The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies and Computer Programs", 84 Harvard L. Rev. 281 (1970); Tyerman, "The Economic Rationale for Copyright Protection for Published Books: A Reply to Professor Breyer", 18 U.C.L.A. L. Rev. 1100 (1971); and Breyer, "Copyright: A Rejoinder", 10 U.C.L.A. L. Rev. 75 (1972).

For a recent discussion of Internet economics see "The economics of the Internet", *The Economist*, October 19, 1996, p. 23.

5 Dixon & Self, "Copyright Protection on the Information Superhighway", [1994] 11 E.I.P.R. 465.

6 There are literally hundreds of books, articles and commentaries worldwide suggesting revisions to the copyright laws in order to accommodate the new era of cyberspace. An incomplete and subjective list of some of the more interesting and provocative ones: Christie, "Reconceptualising Copyright in the Digital Era", [1995] 11 E.I.P.R. 522; Ginsburg, "Putting Cars on the "Information Superhighway": Authors, Exploiters and Copyright in Cyberspace", 95 Columbia L. Rev. 1466 (1995); Hardy, "The Proper Legal Regime for 'CyberspaceÕ", 55 U. of Pitt. L. Rev. 995 (1994).

Those seeking absolute answers concerning potential liability issues will be disappointed with this study. Such certainty is rare even in well-defined areas of the law. In a new and fluid legal landscape such as that relating to copyright infringement on the Internet, the best that can be put forward is an educated guess concerning future legal results based on analogies and analysis of prior cases in other areas. What this study can and does do is attempt to strip away some of the myths and misconceptions surrounding Canadian copyright law and the Internet.

The most glaring of these myths involves the use in Canada of copyright precedents and cases from the United States. Although Canada and the United States share a common law heritage, our copyright law has always been quite dissimilar. Canada has historically been a full participant in in the various international copyright conventions, while the United States has until recently tended to go its own way. The divergence in the approaches of each country has been reflected in differences in their respective copyright laws on issues as fundamental as the need for copyright registration, the term of protection for works, publication and the "first sale doctrine", the concept of "authorization" and indirect infringement (Canada) versus "contributory infringement" (United States) and the exceptions for "fair dealing" (Canada) versus "fair use" (United States). Nevertheless, Canadian courts and commentators continue to regularly cite United States case law in copyright and technology cases.[7]

This problem has become an acute one in connection with the Internet. Every day, papers and commentaries produced by Canadian lawyers, legislators and journalists refer to cases such as *Playboy Enterprises, Inc. v. Frena*,[8] a copyright case in which a BBS sysop was found liable for the posting by users of copyright photographs on the BBS. But the *Playboy* decision was based, at least in part, on contributory infringement by the sysop, a tort concept which is not an accepted rule of Canadian copyright law. Any Internet participant in Canada which bases their understanding of their legal position on the results of cases from the United States might find themselves in for a surprise in the future.[9] Having said this, this study does contain a fairly extensive discussion of the summary judgment motion decision in

---

In Canada, both the Information Highway Advisory Council (IHAC) and the IHAC Copyright SubCommittee have produced reports recommending amendments to the *Copyright Act* to address Internet issues: see "Connection, Community, Content: The Challenge of the Information Highway", Final Report of the Information Highway Advisory Council, September 1995 (the "IHAC Report") and "Copyright and the Information Highway", Final Report of the IHAC Copyright SubCommittee, March 1995 (the "IHAC Copyright Report").

7 See Potter, "Reflections Through a Prism - Case Comment: *Prism Hospital Software Inc. v. Hospital Medical Records Institute*" (1995), 18 B.L.R. (2d) 184.

8 (1993), 839 F. Supp. 1552 (Fla.)

9 Sookman, "Copyright and Technology", in Henderson, *Copyright Law in Canada* (1994), at pp. 288-292.

Religious Technology Center v. Netcom On-Line Communication Services Inc.,[10] at present the seminal judgment on ISP liability for copyright infringement on the Internet.

Another of the difficulties in analyzing Internet copyright liability is the combination of the paucity of case law and the abundance of analogies. When there is no precedent which can be pointed to resolve a particular issue, the natural inclination for legal analysts is to say that the Internet is like something else, or that an Internet participant is just like some other type of copyright participant for which the rules are better defined. The limitations of such an approach to a somewhat related area of computer law were pointed out by Hugessen, J. in *Apple Computer, Inc. v. Mackintosh Computers Ltd.*:[11]

> The principal difficulty which this case has given me arises from the anthropomorphic character of virtually everything that is thought or said or written about computers. Words like "language", "memory", "understand", "instruction", "read", "write", "command", and many others are in constant use. They are words which, in their primary meaning, have reference to cognitive beings. Computers are not cognitive. The metaphors and analogies which we use to describe their functions remain just that.[12]

---

10 U.S.D.C. North. Cal. No. C-95-20091, November 21, 1995 (hereafter "*Netcom*"). While apparently not yet reported, the *Netcom* decision is available on LEXIS and is widely available on several sites on the Internet, including one at http://www.cybercom.net/~rnewman/scientology/erlich/whyte-11.21.95.

11 (1986) 28 D.L.R. (4th) 178 (F.C.T.D.); varied (1987) 18 C.P.R. (3d) 129; aff'd (1990) 30 C.P.R. (3d) 257 (S.C.C.).

12 (1987) 18 C.P.R. (3d) 129 (F.C.A.), at p. 140. See also Sookman, "Copyright and Technology", in Henderson, *Copyright Law in Canada* (1994), at pp. 287-288. For an amusing commentary on the overuse of "cyberlingo" such as "information superhighway", see Allard, "Copyright from Stone Age to the Celestial Jukebox", 17 Hastings Comm/Ent. L.J. 867 (1995), at pp. 868-869:

> "The patron saint of English language watchdogs, Sir Winston Churchill, once rose up in the House of Commons to ridicule an opposition politician merely for using the word "infrastructure" in parliamentary debate. Today, standing up to empty communications jargon in Congress would amount to aerobic exercise."

In Alben, "What is an On-line Service? (In the Eyes of the Law)", 6-13 *Computer Lawyer* 1 (June 1996), the author compares on-line services to publishers, dance halls, libraries and bookstores, printing presses, common carriers and shopping malls and concludes that on-line services and Web sites are a hybrid of characteristics of all of these things. In Dunstan & Lyons, "Access to Digital Objects: A Communications Law Perspective", *1994 Annual Survey of American Law* 363, ISPs are analogized to banks and broadcasters.

This study will try to avoid the "analogy trap" (at least to the extent possible) by concentrating on basic copyright principles and their application to the specific Internet application being examined.

In summary, this study attempts to state current Canadian copyright law as it applies to liability for infringement as a result of content transmission on the Internet. While reference will be made to legislative and judicial decisions in other countries, it is hoped that this study will serve as a guide to understanding how our Canadian legal system can cope (or in some cases not cope) with the challenges of the Internet.

2. THE BASICS OF CANADIAN COPYRIGHT LAW

Because this study is intended to deal primarily with liability issues, there are a number of elements of Canadian copyright law which are dealt with only very briefly. These include the types of works which attract copyright and the authorship and ownership of such works.

(a) Creation of Copyright Works

Although this study is not directly concerned with the issue of whether material transmitted on the Internet is copyrightable,[13] it is useful to describe generally how copyright in works arises and to describe the types of works that might appear on the Internet.

Copyright exists in "works", which must have some corporeal existence. Once a work is created, copyright in the work subsists in Canada if the following conditions are satisfied:

(a) Section 5 of the *Copyright Act* requires that the author of the work satisfy certain citizenship or residence requirements, which basically require that the author is a citizen of, or resident in, a "treaty country"[14] or in the case of a published work, its first publication must be in such a quantity as to satisfy the reasonable demands of the public and have occurred in a treaty country.[15] The author and residence requirements can make Internet copyright infringement claims difficult to prove if there are a number of authors from different countries.

(b) The work must be "original". In addition to requiring that the work not be simply a copy of another work, this requirement means that the work must be the product of some sufficient skill, labour or judgment, and that it must be more than simply an idea or information with little or no expression.[16]

---

13 For an example of this type of dispute, see "Big bucks on line in Internet battle", Toronto *Star*, September 18, 1996, page D3, dealing with the dispute between the owners of sports franchises and Internet entrepreneurs providing "instant" game updates and scores.

14 Protection can be extended to other countries by the Minister pursuant to Section 5(2). A "treaty country" is defined in Section 2 to mean a country which has joined either of the Berne Convention, the Universal Copyright Convention or is a member of the World Trade Organization.

15 Section 5(c).

16 See Hayhurst, "Copyright Subject-Matter" in Henderson, *Copyright Law of Canada* (1994), at pp. 41-48.

There are interesting issues raised by the "originality" requirement as it applies to works on the Internet. Much of the communication on the Internet may not be "original" since it is simply informational (in the case of simple e-mail communications or advertising descriptions, for example) or consists of ideas without expression (many chat sessions and newsgroup messages could not be described as much more than digital speaking).[17]

In the recent *Tele-Direct* case,[18] the Federal Court held that Tele-Direct did not have copyright in the compilation of information contained in the various "Yellow Page" directories published across Canada. This decision could affect copyright protection for databases and other information compilations available on the Internet.[19]

The *Copyright Act* defines four types of copyright work: literary, dramatic, musical and artistic. It is intended that every type of work subject to copyright protection will be included within one or more of these categories.[20] For example, computer software has been classified as a literary work, even though at first impression most software would not strike the casual observer as literary.[21] There are also several defined sub-categories of copyright works, such as architectural works and cinematographs.

The classification of a work may have some importance to the question of infringement. Some types of infringement are defined to apply only to certain categories of works. For example, Section 3(1)(d) grants an exclusive right to make records "or other contrivances" of literary, dramatic or musical works, but excludes artistic works. It is theoretically possible, therefore, that there is no need to obtain the consent of the owner of the copyright in an artistic work before making a digital record of it; it would appear,

---

17 During one of the focus group sessions in connection with this study, which was discussing collectives and Internet royalties, a participant pointed out that the vast majority of information on the Internet was placed there without any expectation of compensation, but that as soon as a collective were to be formed to collect Internet royalties, everyone with a Web page would want to be compensated for the "hits" to it. It is quite likely that a substantial amount of the material on the Web would not pass the test of originality in order to qualify for copyright protection and payment of such royalties.

18 *Tele-Direct (Publications) Inc. vs. American Business Information Inc.* (1996), 113 F.T.R. 123, 27 B.L.R. (2d) 1 (F.C.T.D.).

19 There was an interesting Internet issue in the *Tele-Direct* case in that the defendant ABI offered a database access service over the Internet from its main office in Nebraska to subscribers in Canada. The issue thus arose as to whether the availability of copyright material in an American database which was available to be accessed by Canadian subscribers could be copyright infringement in Canada. As a result of the decision that the ABI database and publications did not infringe Tele-Direct´s copyright, the Internet issue was not decided. This issue of international infringement on the Internet is discussed later in this report.

20 At least one author has suggested that the ability to create interactive linked works with hypertext has created a new type of work: see Georgini, "Through Seamless Webs and Forking Paths: Safeguarding Author's Rights in Hypertext", 60 Brooklyn L. Rev. 1175 (1994).

21 Sookman, "Copyright and Technology", in Henderson, *Copyright Law in Canada* (1994), at pp. 292-295.

however, that the reproduction right for an artistic work might still be infringed in such an instance.

Many Internet transmissions, especially on the World Wide Web,[22] will include a number of different types of works compiled together. While the analysis in this report focuses on the transmission of single works in determining whether there has been infringement, it must be remembered that each element of an Internet transmission may have to be examined separately to determine whether copyright has been infringed.

(b) Authorship

One of the basic concepts of copyright is authorship. The initial owner of copyright in a work is the author of the work, although the author may subsequently assign all or part of the copyright.

One of the difficult issues on the Internet involves collaborative works and work of joint authorship. With the proliferation of Usenet and various chat networks, many creative people are using the Internet to find other authors and artists to work with them on projects and the creation of collaborative works such as scripts, story treatments and creative designs and ideas. If the collaboration turns into a commercially saleable work, there may be controversy concerning who is the author of the completed work.[23]

Section 2 defines a "work of joint authorship" as a work "produced by the collaboration of two or more authors in which the contribution of one author is not distinct from the contribution of the other author or authors".[24] Generally, each of the authors of a work of joint authorship is entitled to full copyright in the work, which essentially means that the work must be exploited by all of the joint authors or none at all. This appears to be different from the situation in the United States, where a co-owner of a copyright work cannot be liable for infringement of copyright in relation to another owner, and each party has the independent right to use or license the work subject only to a duty to account.[25]

---

22 For a brief history of the Web, see http://www.w3.org/pub/WWW/History.html.

While this issue is by no means a new one, the increased potential and ease of collaboration on the Internet have highlighted the possibility for conflicts among collaborating authors: see Ginsburg, "Putting Cars on the "Information Superhighway": Authors, Exploiters and Copyright in Cyberspace", 95 Columbia L. Rev. 1466 (1995), at pp. 1469-1472 and Georgini, "Through Seamless Webs and Forking Paths: Safeguarding Author's Rights in Hypertext", 60 Brooklyn L. Rev. 1175 (1994), at pp. 1187-1191.

24 A work of joint authorship must be contrasted with a compilation in which several authors combine their individual and distinct works into a new work. In the case of a compilation such as a multi-media work or a feature film, the individual authors may continue to separately own the component works while they all have joint ownership of the compilation. In a work of joint authorship, there is no separate work and no author can claim ownership of any distinct part of the work.

25 Mann, "Acquisition, Ownership and Collective Administration of Copyright", in Henderson, *Copyright Law of Canada* (1994), at pp.103-104.

The increasing use of "robots" on the Internet also raises questions of authorship. A robot crawler may be designed to visit millions of Web sites and gather information for an on-line index or book of addresses.[26] If the work compiled by that gathering of information is entitled to copyright protection, who is the author of the work? In principle, it would appear that the person that instructed the crawler to do the search would be the author, rather than the creator of the crawler or its owner, since the crawler was merely the instrumentality by which the person created the work, but this is far from clear.[27]

(c) Ownership of Copyright Works

Canadian copyright law permits the owner of the copyright in a work to assign or license all or a part of the copyright, either generally or subject to territorial or use limitations. An assignment of copyright must be in writing,[28] but a license can be implied from the custom of the trade.[29] Moral rights can not be assigned, but may be waived.[30]

Recent controversy has arisen over ownership of Internet rights to existing works. Freelance authors in both the United States[31] and Canada[32] are suing newspaper and magazine publishers for copyright infringement. The authors claim that they did not assign the rights to exploit their articles on the Internet, and that their copyright was infringed when the publishers began to place these articles on Web sites and on-line archives.

---

26 See "New engine can index entire Web each week", Toronto *Star*, September 5, 1996, p. J3.

27 Sookman, "Copyright and Technology", in Henderson, *Copyright Law in Canada* (1994), at pp. 295-300.

28 Section 13(4). Similar provisions apply to performers' rights: see Section 14.01(6) and 13(4).

29 See *Hughes on Copyright and Industrial Design* (1984), at p.446.

30 Section 14.1.

31 Jonathan Tasini, the President of the National Writers Union, and others have sued the *New York Times* and other newspapers and periodicals claiming damages for the placing of the works of freelance writers into on-line services run by the defendants. The plaintiffs' position is set out at http://www.nwu.org/nwu/tvt/tvtcopyr.htm. For a detailed description of the legal basis of the American dispute, see Rosenzweig, "Don't Put My Article On-line!": Extending Copyright's New-Use Doctrine to the Electronic Publishing Media and Beyond", 143 U. of Penn. L. Rev. 899 (1995).

32 Heather Robertson has launched a class action suit against Thomson Corporation, the publisher of the Toronto *Globe & Mail*, claiming $100 million in damages for the use of articles by freelance writers in on-line applications. Information on the Robertson suit is posted from time to time on the Web page of the Periodical Writers Association of Canada at http://www.cycor.ca/PWAC.

Because the primary focus of this report is on copyright infringement rather than copyright ownership, an analysis of this issue is beyond the scope of this report, but it should be noted that this type of dispute is not new. Every major development in the exhibition or exploitation of creative works has spawned a dispute about whether pre-existing contracts by which the copyright owner has licensed the work also encompasses new technologies.[33] In addition, it is likely that the publishers will claim an implied license to permit use of the freelancers' work for all purposes, and the resolution of this issue will be of great interest to all Internet participants.[34]

---

33 See Skone James, *Copinger and Skone James on Copyright* (13th ed., 1991), at pp. 126-127.

34 See *Cselko Associates Inc. v. Zellers Inc.* (1992), 44 C.P.R. (3d) 56 (Ont. Ct. (Gen .Div.)) and *Allen v. Toronto Star Newspapers Ltd.* (1995), 63 C.P.R. (3d) 517 (Ont. Ct. (Gen.Div.)). Implied licenses are discussed later in this report.

3. INTERNET COPYRIGHT INFRINGEMENT IN CANADA

In order to determine the nature of potential copyright infringement in Canada as a result of the unauthorized use of copyright materials on the Internet, it is necessary to first consider two basic questions:

(a) Which, if any, of the rights granted to copyright holders by the *Copyright Act* can be infringed on the Internet?

(b) Under what circumstances could such an infringement take place in Canada so as to fall within the scope of the *Copyright Act*?

Answering these two questions requires both an analysis of several aspects of current Canadian copyright law and of its potential application to the Internet environment.

(a) Rights Infringed on the Internet

Copyright is a statutory creation. It is neither contract nor tort law, and reference to such common law regimes is of limited assistance in copyright cases.[35] Further, Section 63 of the *Copyright Act* provides that "no person is entitled to copyright or any similar right in any literary, dramatic, musical or artistic work otherwise than under and in accordance with this Act".[36] As a result, in order to determine whether there is copyright infringement on the Internet, it is necessary to first examine carefully what exclusive rights are granted by the *Copyright Act* to copyright owners.[37]

Section 3 of the *Copyright Act* contains an exhaustive listing of the "sole

---

35 *Compo Co. v. Blue Crest Music Inc.*, [1980] 1 S.C.R. 357 at 372; *Télé-Métropole Inc. v. Bishop*, [1990] 2 S.C.R. 467 at 477; *Delrina Corp. v. Triolet Systems Ltd.* (1993), 47 C.P.R. (3d) 1 (Ont. Ct. (Gen. Div.)) at 27.

36 Section 63 appears to be intended to preclude any argument that a "common law" copyright exists: see *Hughes on Copyright and Industrial Design* (1984) at pp. 321-322.

37 While it is beyond the scope of this study to examine potential remedies for Internet copyright infringement, it is important to note the "statutory damages" provisions contained in Bill C-32 (Section 38.1). This section permits the copyright owner to elect to receive damages of from $500 to $20,000 for each work infringed instead of having to prove actual damages. The court is given some discretion to award a lower amount in specific circumstances. With the potential for instantaneous and simultaneous infringement by transmission of numerous works over the entire Internet, one must ask both whether the statutory damages specified are too high (since an individual user could be liable for many thousands of dollars in respect of a short newsgroup session, even when the copyright owner suffers no damage whatsoever as a result) or too low (considering that unlimited copies of a work can be transmitted all over the world, and the statutory damages limit is $20,000 for all infringements alleged in respect of a single work).

rights" which are granted to copyright owners. Those which might be relevant to the Internet include the exclusive right to do or authorize[38] any of the following acts:

(a) produce or reproduce the work or any substantial part of the work "in any material form whatever" (Section 3(1));

(b) perform in public the work or any substantial part of the work (Section 3(1));

(c) publish all or a substantial part of an "unpublished" work (Section 3(1));

(d) produce, reproduce, perform or publish any translation of a work (Section 3(1)(a));

(e) convert a dramatic work into a non-dramatic work (Section 3(1)(b));

(f) convert a non-dramatic or artistic work into a dramatic work (Section 3(1)(c));

(g) make any record "or other contrivance" of a literary, dramatic or musical work "by means of which the work may be mechanically performed or delivered" (Section 3(1)(d));

(h) reproduce, adapt or publicly present a cinematograph (Section 3(1)(e));

(i) communicate a literary, dramatic, musical or artistic work to the public by telecommunication (Section 3(1)(f));

(j) reproduce, publish or rent a record "or other contrivance" by means of which sounds may be mechanically reproduced (Section 5(4)).[39]

There is some question whether the retention of a copy of the copyright work on a mail server or a recipient's hard drive is either a making of a "record ... by means of which the work may be mechanically performed or delivered" within the meaning of Section 3(1)(d) or the reproduction, publication or rental of a record "or other contrivance" by means of which sounds may be mechanically reproduced within the meaning of Section 5(4). Although it seems from the context of Section 3(1)(d) that these provisions are intended to deal with physical recordings such as CDs and videotapes, the sections themselves are not clearly limited in this way and there seems to be no distinction in principle between computer

---

38 See the discussion of the concept of "authorization" in the following section on direct infringement.

39 It can be argued that there are other rights which could possibly be infringed on the Internet, including the computer program rental right (Section 3(1)(h)) and the public presentation right in respect of an artistic work (Section 3(1)(g)). Because the rights already enumerated clearly cover the spectrum of uses on the Internet, the consideration of these more speculative rights add little to the analysis.

storage media and more "portable" recording formats.[40] Because there is no practical distinction between acts which could infringe the reproduction right and those acts which could infringe the rights created by Section 3(1)(d) and Section 5(4), this report will focus only on the reproduction right.

Section 27 of the *Copyright Act* also provides that certain uses of copyright material are defined to be infringement if there is the required level of knowledge on the part of the alleged infringer. These uses are generally, but not exclusively, commercial uses, and include:

(a) sale or lease of a work, or the exposure or offer for sale or hire of a work, "by way of trade";

(b) distribution of a work for the purposes of trade or "to such an extent as to affect prejudicially the owner of the copyright";

(c) exhibition of a work in public by way of trade; or

(d) importation of the work into Canada for sale or hire.

In order for there to be infringement in each of the instances enumerated in Section 27, there must be knowledge on the part of the infringer that the work infringes copyright or would infringe copyright if it had been made in Canada.[41]

In addition, pursuant to Section 14.1 of the *Copyright Act*, the copyright owner is entitled to certain moral rights, including the right to integrity of the work and the right to be associated with the work as its author (or alternatively to remain anonymous).

In 1994, amendments to the *Copyright Act* have also given certain exclusive rights to performers in live performances that are either communicated to the public by

---

40 As noted above, in the *Télé-Métropole* case, McLachlin J. did not distinguish between the reproduction right set out in Section 3(1)(a) and the right to make a "record ... or other contrivance" set out in Section 3(1)(d). The defendant was found to have made a "record" when it retained a videotape of the performance of the plaintiff's work. There does not appear to be any reason why, in an appropriate case, the making of a "record" cannot also be a reproduction.

41 It is unclear whether indirect infringement pursuant to Section 27(4) is limited to tangible copies of copyrighted works or can be apply to dealings with digital copies as well. The context of the specific actions enumerated, in particular the reference to importation in subparagraph (d), would seem to indicate that Section 27(4) is intended to refer to tangible copies. However, there is nothing in Section 27(4) to indicate that, in appropriate circumstances, a digital "distribution" or "sale" could not be interpreted to fall within the provision. Indirect infringement is discussed in more detail in the next section of this report.

telecommunication or recorded.[42]

It will immediately be apparent that what would normally be seen by a user of the Internet as a single act (for example, downloading a Web page) may in fact potentially involve the infringement of several of the exclusive rights set out above. There may be both a communication to the public by telecommunication and a reproduction of a work, all done more or less simultaneously. In addition, the work may have been altered so as to infringe the author's moral rights. Under the current Bill C-32 proposals, a Web communication may also be an unauthorized communication to the public of a live performance. Many separate copyright works may be included in any individual Internet transmission and the rights of the owners of each of the works may be infringed individually in differing ways.

The *Copyright Act* does specify certain exclusions which would prevent some of these potential multiple infringement scenarios. In particular:

(a) the communication of a work to the public by telecommunication is neither a performance in public nor the authorization of a performance in public (Section 3(4))[43]; and

(b) the definition of publishing excludes performances in public and the communication of the work to the public by telecommunication (Section 4(1)).

The focus of the Canadian *Copyright Act* is on activities which infringe copyright. This is to be contrasted with the copyright statute in the United States which has tended to identify specific classes or categories of persons who are deemed to be either infringing or exempted in certain specific circumstances.[44] There are advantages to the Canadian approach in that a flexible definition of infringing activities can often be adopted to

---

42 Sections 14.01 and 28.02. While neither moral rights nor performers' rights are technically copyrights, they are generally discussed at the same time as copyright as a result of the similar terminology employed and because of their inclusion in the *Copyright Act*. It is important to note that the scope of moral rights and performers' rights are considerably narrower than copyright: see *Hughes on Copyright and Industrial Design* (1984) at pp. 638-641.

43 The amendments to the *Copyright Act* proposed in Bill C-32 make it clear (in the new Section 2.3) that a communication of a work to the public by telecommunication of a work to the public by telecommunication does not "by that act alone" perform the work in public. If, however, a further step is taken at the end of the communication, such as the showing of the work to a large gathering of unrelated people, this could constitute both a communication to the public and a performance in public. This is likely the current law in any event as a result of the decision of the Supreme Court of Canada in *Télé-Métropole Inc. v. Michel Bishop*, [1990] 2 S.C.R. 467.

44 For example, sections 111 (secondary transmissions and cable services), 112 (ephemeral recordings), 116 and 116A (jukeboxes), 118 (non-commercial broadcasting) and 119 (direct-to-home satellite broadcasts) of the United States *Copyright Code* all contain very detailed provisions targeted at specific technologies and users.

new technologies such as the Internet. Conversely, it may make it difficult to easily establish infringement when new technologies lead to new activities which affect the rights of copyright owners.

It is important for a number of reasons to identify which of the exclusive rights detailed above are being infringed by Internet communications. First, as is discussed in more detail below, there may be defences available for some categories of infringement but not others. An example is the exemption set out in Section 3(1.3) of the *Copyright Act*, which provides that a person does not communicate a work to the public where the person's "only act in respect of the communication of a work to the public consists of providing the means of telecommunication necessary for another person to so communicate the work". If, however, the transmission is also a reproduction, the exemption contained in Section 3(1.3) does not apply in respect of that infringement of the reproduction right.[45]

Secondly, copyright in a work is by agreement often split amongst several rights holders. A composer and publisher of a musical work will generally assign performance and telecommunication rights and mechanical (recording) rights to separate collectives. A music publisher often will own the rights to the written representation of the notes and words contained in the work. There may also be a record company or producer which owns a separate copyright in the sound recording of a performancs of musical work.[46] As a result, if there is in fact liability for copyright infringement on the Internet, it will be necessary to determine which rights are being infringed in order to identify which rights holder or holders can assert a claim for copyright infringement, attempt to collect royalties or have standing in the courts to take steps to stop the infringement.[47]

In order to assess the nature of copyright infringement on the Internet, some common Internet transactions must be analyzed. These transactions can be broken down into two main categories: (i) e-mail and newsgroups and (2) World-Wide Web, FTP and BBSs.[48]

---

45 In *Télé-Métropole Inc. v. Michel Bishop*, [1990] 2 S.C.R. 467, which is discussed in more detail below, the defendant had a license to broadcast the work, but not to record it. When the work was recorded by the broadcaster in the course of the broadcast, the broadcaster was held to have infringed the recording right in Section 3(1)(d). The same logic should apply in a situation where a party is entitled to the exemption pursuant to Section 3(1.3) but has also infringed the recording or reproduction right.

46 The *Copyright Act* is somewhat limited in the protection currently offered to sound recordings. The proposed amendments in Bill C-32 will define sound recordings, make it an infringement of the sound recording owner's copyright to make any copy of the recording, include sound recordings within the definition of performance and define the making of a sound recording available to the public as a publication of the sound recording.

47 See Segal, "Dissemination of Digitized Music on the Internet: A Challenge to the Copyright Act", 12 Santa Clara Comp. & High Tech. L.J. 97 (1995), at pp. 113-120 for a discussion of this issue under United States copyright law.

48 This rough division does not encompass some types of Internet communications such as Internet Relay Chat sessions. It is unlikely that significant amounts of copyright material would be transmitted in an IRC session. In any event, the concepts discussed in respect of these two broad categories can be easily applied to other Internet communications.

(i) E-Mail and Newsgroups

Electronic mail remains by far the most common use of the Internet. A single user originates a message, which is delivered to one or more users on the Internet. The message may be text only or may attach other files which could contain text, software, pictures, videos or music.

Newsgroups must be considered along with e-mail because they are similarly message-based. Newsgroups involve the public posting of a sender's message (and any attached documents) in one or more of thousands of newsgroup categories. Persons interested in that category may examine some or all of the posted messages and may respond to them. Responses may be made by posting a responding message to the newsgroup or by sending an e-mail message to the user who posted the original message.

The simplest example of a potential infringement is of an individual e-mail message sent from one individual user to another and which contains or attaches copyright material owned by a third party which has not licensed its use. The sending user instructs its mail software to send the message to the recipient's e-mail address. The mail software then sends a copy of the work to the sending user's ISP's mail server. That ISP then transmits the packets which make up the e-mail message to the receiving user's ISP's mail server. Along the way, the individual packets may take a variety of routes to reach the ultimate destination. The receiving user's ISP assembles the various packets as they are received until the entire message is available. The assembled message is then stored on the ISP's mail server until the receiving user accesses the message and downloads it to the user's computer from the mail server.

The transmission of an Internet e-mail message is a "communication by telecommunication" within the meaning of Section 3(1)(f) of the *Copyright Act*. "Telecommunication" is widely defined in Section 2 to mean "any transmission of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual, optical or other electromagnetic system". It is clear that the intention of the *Copyright Act* is to encompass every form of electromagnetic or wireless communication within this definition.

E-mail is, however, different from a telephone call or a television broadcast (both classic examples of "communication by telecommunication") in that there is not a single direct communication from the sender to the recipient. An e-mail message is sent by the sender to a server, the server sends the message to the recipient's server, and the recipient downloads the message.[49] It is unclear whether this is one communication (ie. from the

---

49 This is, of course, the minimum number of steps involved. There may be various remailers interposed along the way.

sender to the recipient) or a series of communications from one stage of the e-mail process to the next.[50]

As will be seen later in this report, this is not an insignificant issue. If the communication is seen as being from the sender to the recipient, Internet intermediaries likely could not be communicating with anyone when their equipment in systems are employed by users to send messages. If in fact the intermediary is seen to be sending or receiving the communication, this could increase its potential liability.[51]

The fact that an e-mail message containing an unauthorized copyright work may be a communication by telecommunication is not, however, sufficient to constitute copyright infringement since Section 3(1)(f) grants a right of communication "to the public". The *Copyright Act* contains no prohibition on a communication of a copyright work by telecommunication as long as the communication is not "to the public".[52] It must therefore be considered whether e-mail and newsgroup messages are being communicated "to the public" such that the right to communicate to the public by telecommunication is being infringed.

"To the Public"

The Information Highway Advisory Council (IHAC) Copyright SubCommittee expressed the opinion that "point-to-point e-mail between two individuals, even where it includes a copyright work, is not a communication of that work to the public".[53] While e-mail between two persons (or some other very small number of individuals) is "private" (or at least is not "to the public"), at some point the number of recipients of an e-mail will become so large that the communication becomes "to the public". However, this was not explicitly discussed, and no distinguishing point was suggested between those communications which

---

50 See Loundy, "Revising the Copyright Law for Electronic Publishing", 14 J. of Comp. & Info. Law 1 (1995), at pp. 26-31.

51 The right of "communication to the public by telecommunication" granted by Section 3(1)(f) seems to be unique in that it is the only exclusive right which is granted by the *Copyright Act* which can be accomplished through the use of an intermediary carrier such as a telephone company, cable operator or ISP. It appears that the only infringing activities which a carrier of physical goods could be seen to be involved in would fall under the definition of indirect infringement in Section 27(4). For example, the delivery of a number of infringing copies by mail could be seen to be either a distribution to the public within the definition of Section 27(4)(b) or an importation under Section 27(4)(d). In both of these circumstances, a carrier such as Canada Post could not be liable since it would not in the normal course have the requisite knowledge required by Section 27(4). See Heinke and Rafter, "Rough Justice in Cyberspace: Liability on the Electronic Frontier", Computer Lawyer, July, 1994, at 1.

52 The "public/private" dichotomy is a common dividing line which attempts to achieve a balance between the rights of copyright owners and the avoidance of intrusion in the privacy of users: see Geller, "Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked World", 20 Columbia - ULA J. of Law & the Arts 571 (1996), at p. 593.

53 IHAC Copyright Report, p. 10. As is discussed below, it is arguable that some point-to-point e-mail communications are "to the public" if made in commercial contexts.

are "to the public" and those which are not.

Historically, wireless communication was dealt with under the "performance in public" right until the amendments to the *Copyright Act* in 1994 made it clear that all communications by telecommunication were no longer to be considered performances. As a result, there is a considerable body of Canadian case law which deals with the phrase "in public" as it relates to broadcasting, but as of yet no cases dealing with the phrase "to the public". Some guidance to the meaning of "to the public" can be gained, however, from a review of the public performance decisions.

The well-known case of *Canadian Admiral Corp. Ltd. v. Rediffusion Inc.*[54] involved a dispute over television broadcasts of football games. Canadian Admiral had purchased the right to broadcast telecasts of the football games. Rediffusion was what would be known today as a cable operator. Without the permission of Canadian Admiral, Rediffusion had taken the television signals of the games broadcast by the licensees of Canadian Admiral and communicated them to Rediffusion's subscribers.

In considering whether Rediffusion had performed the contested works "in public", the Exchequer Court applied a "character of the audience" test and found that the communication by Rediffusion was not "in public". In doing so, the Court considered a line of English cases dealing with public performances in clubs, hotels and other public places[55] and held:

> "In none of these cases, however, can I find a suggestion that a performance in a private home where a performance is given, heard or seen by only members of the immediate household, could be considered as a performance in public.
>
> As to the character of the audience in homes and apartments to which the telecasts of the live films were "rediffused" by the defendant, there is no evidence whatever except that they were seen by the defendant's subscribers, presumably only the householders. The character of the audience was therefore a purely domestic one and the performance in

---

54 [1954] Ex. C.R. 382.

55 *Duck v. Bates* (1884), 13 Q.B.D. 843; *Harms Inc. v. Martan's Club*, [1927] 1 Ch. 526; *Performing Right Society Ltd. v. Hawthorne's Hotel (Bournemouth) Ltd.*, [1933] 1 Ch. 856; *Jennings v. Stephens*, [1936] 1 All E.R. 409; *Performing Rights Society Ltd. v. Gillett Industries Ltd.*, [1943] 1 All E.R. 228 and 413.

> each case was not a performance in public. Counsel for the plaintiff, however, submits that even if one such "view" in the privacy of the owner's home does not constitute a performance in public, that in cases where a large number of people, each having a terminal unit in his home, performs the work by operating the terminal units, that such would constitute a performance in public. He says that from the point of view of the owner, a large number of such performances would constitute an interference with the owner's right of making copies of his work and might cause him to lose part of his potential market. I am unable to agree with that submission. I cannot see that even a large number of private performances, solely because of their numbers, can become public performances. The character of the individual audiences remains exactly the same; each is private and domestic, and therefore not "in public"."[56]

The decision in the *Rediffusion* case took a very strict view of the scope of copyright protection for works transmitted into private homes. It is possible that the relatively novel nature of television in the early 1950s contributed to this approach.

The Federal Court of Appeal had occasion to revisit this issue in *Canadian Cable Television Association v. Copyright Board ("CCTA").*[57] *CCTA* involved an application to prevent the Copyright Board from considering a music performance tariff which sought to fix the CCTA's cable operator members with liability to pay royalties in respect of musical works contained in "non-broadcast" cable services transmitted to subscribers by CCTA members. The Federal Court of Appeal overruled the *Rediffusion* decision and held that CCTA's members were performing musical works in public:

"In *Chappell Co. v. Associated Radio Co. of Australia Ltd.*[58] Cussen J. wrote for the Court (at p. 362):

> "A performance, in our judgment is no less public because the listeners are unable to

---

56 *Rediffusion* , *supra*, at p. 407.
57 (1993), 46 C.P.R. (3d) 359.
58 [1925] V.L.R. 350.

> communicate with one another or are not assembled within an enclosure or gathered together in some open stadium or park or other public place. Nor can a performance, in our judgment, be deemed private because each listener may be alone in the privacy of his home. Radio-broadcasting is intended and in fact does reach a very much larger number of the public at the moment of the rendition than any other medium of performance."

This is certainly even truer of a transmission by means of television. I am satisfied that the transmission of non-broadcast services by the appellant to its numerous subscribers, when it relates to musical works, is a performance in public within the meaning of s. 3(1) of the *Copyright Act*."[59]

Subsequent amendments to the *Copyright Act*[60] have made it clear that cable television transmissions are communications to the public by telecommunications and not public performances.[61] No case in Canada has yet dealt definitively with the difference, if any, between the words "in public" used in relation to performances and the words "to the public" used in relation to communications by telecommunication. The Federal Court of Appeal, in both the *CCTA* case and its companion case *Performing Rights Organization of Canada Ltd. v. CTV Television Network Ltd.*[62] ("*CTV*"), was willing to accept, without deciding, that the words "to the public" are broader than "in public".[63]

In the *CTV* case, the Federal Court of Appeal held that the CTV Network did not perform musical works in public when it transmitted its programming to its affiliate stations. The Court relied in part on the fact that CTV was licensed by the CRTC only as a programmer, and not as a broadcaster, and therefore had no authorization from the CRTC to broadcast to the public.[64] It would appear that such a distinction breaks down when applied to the Internet, since no attempt has yet been made to either classify Internet transmissions as "broadcasting" or to license Internet transmitters.[65]

---

59 *CCTA*, at p. 371.

60 S.C. 1993, c. 44.

61 "This change in the statute may effectively bring the law back to the result expressed in *Canadian Admiral v. Rediffusion*, [1954] Ex.C.R. 382, that the simultaneous "rediffusion" of a work by cable television to a number of private residences was not a performance of the work in public": *Hughes on Copyright and Industrial Design* (1984) at p. 547.

62 (1993) 46 C.P.R. (3d) 343.

63 *CCTA*, at p. 367; *CTV*, at p. 354.

64 *CTV*, at p. 358.

65 As this report is being written, there are increasing signs that the CRTC is preparing to attempt to assert at least limited jurisdiction over the Internet: see "CRTC considers regulating Internet", Toronto Star, November 15, 1996, p. A13 in which CRTC chair Fran_oise Bertrand is quoted as saying that "But one

The determination of whether a communication by telecommunication is "to the public" will likely depend on whether the communication is made "openly, without concealment"[66] to a sufficiently large number of recipients. No case has attempted to quantify a specific cut-off point.

In Australia, the definition of "to the public" was considered in *Australasian Performing Rights Society v Telstra Corporation Ltd.*[67] In that case, the plaintiff music collective had claimed that the telephone company defendant had infringed the collective's copyrights when it transmitted music on hold during telephone communications. The Federal Court of Australia held, based on the wording of the *Copyright Act 1968 (Cth)*, that there was no infringement by the telephone company.[68] One of the claims made was that music on hold during cellular telephone transmissions was "broadcast". The definition of broadcast was to "transmit by wireless telegraphy to the public". Not surprisingly, the Federal Court found that, because the cellular telephone service is intended to communicate a message from one person to another by wireless means, cellular transmissions were not "to the public" and could not constitute broadcasting. Interestingly, after reviewing the older cases dealing with performances "in public", the Federal Court was of the opinion, in an *obiter* passage, that the phrase "to the public" "may involve a more restrictive meaning than the phrase "in public"".[69] The Court did not elaborate on its reasons for reaching this conclusion, which conflicts with the *obiter* observations of the Federal Court of Appeal in the *CCTA* and *CTV* cases.

In the case of e-mail transmissions, it may be that the method by which the recipients are selected will be determinative. For example, an e-mail mailing list compiled by an individual over time may still be private despite the number of recipients. The fact that the sender has had to individually choose each recipient might lend the communication a "private" nature. In contrast, a broadcast message to all persons with e-mail addresses with a specific suffix (such as "uoft.ca") would appear to be "public" since the sender is targeting a wide group of recipients who have not been individually identified. Such a "public" broadcast message might very well be directed to fewer recipients than a "private" e-mail message sent to a large mailing list by an individual. The Supreme Court of Canada has held, in another

---

thing I know is, certainly, from the start, to say there is no place, or no role, for the CRTC is certainly not in my mind". This issue of whether some or all of the Internet is "broadcasting" or within the scope of CRTC regulation is beyond the scope of this study: see Hayes, "Canada, Cultural Sovereignty and the Internet", 1-4 *Cyberspace Lawyer* 13 (1996).

66 *CCTA*, p. 370.

67 [1994] R.P.C. 299 (Fed.Ct.)

68 It is interesting to note that SOCAN's Tariff 15.B relating to music on hold is directed at the trunk line owner, not the telephone company. While the position of the trunk line owner was not considered in *Telstra*, comments by the Federal Court would indicate that it would not have found the trunk line owners liable either.

69 *Telstra, supra*, at p. 314. It would be interesting to speculate what would happen if the cellular call were a conference call to several unrelated people and music on hold was played to all of them. The Federal Court noted at p. 13 of its decision that there was no evidence that any of the cellular calls in issue involved more than one person on the same line.

context, that "it is the originator's state of mind that is decisive" in determining whether a communication is "private".[70]

It is also likely that commercial e-mail would be far more likely to be seen as "to the public". A commercial operator sending e-mail to 100 potential customers on a mailing list compiled by an Internet service and purchased for a fee would be much more likely to be found to be engaged in communication "to the public" than an individual sending e-mail to 100 friends and family members.[71]

The intellectual property provisions of the North American Free Trade Agreement (NAFTA) support the "friends and family" concept of private communications. Article 1721(2) defines "public" as follows:

> "public includes, with respect to rights of communication and performance of works provided for under Articles 11, 11bis(1) and 14(1)(ii) of the Berne Convention, with respect to dramatic, dramatico-musical, musical and cinematographic works, at least, any aggregation of individuals intended to be the object of, and capable of perceiving, communications or performances of works, regardless of whether they can do so at the same or different times or in the same or different places, provided that such an aggregation is larger than a family and its immediate circle of acquaintances or is not a group comprising a limited number of individuals having similarly close ties that has not been formed for the principal purpose of receiving such performances and communications of works."

This definition has not been incorporated into the *Copyright Act*, and, although influential in interpreting the *Copyright Act*, is not binding in Canadian law until it is so incorporated.[72]

BBS or Web page operators will sometimes place samples of copyright materials on their servers and take orders for copiesof works which are then communicated to customers by individual e-mail messages. Such e-mail may be "to the public", despite the one-to-one nature of the communication, since it is merely a continuation of the commercial

---

70 *Goldman v. The Queen* (1979), 108 D.L.R. (3d) 17 (S.C.C.), at p. 30. It would therefore appear that it is the intention of the sender of the message which is determinative of the private or public nature of the message.

71 The increasing use of technological tools to compile e-mail mailing lists will make such lists easily available for specialized marketing and other purposes. It is most unlikely that communications to pre-packaged lists of this sort could be seen as anything but "to the public".

72 See, for example, *Milliken & Co. v. Interface Flooring Systems (Canada) Inc.* (1994), 68 C.P.R. (3d) 157 (F.C.A.).

communication to the public initiated through the BBS or Web site.

At the other end of the private/public spectrum are newsgroups. By their very nature, the posting of a message to a newsgroup involves a potential communication to an undetermined number of persons not known to the sender. The intent of the person posting the message is to provide access to its contents to any member of the public which wants to copy the message's contents and there can be no expectation of privacy by the poster that the communication will be private.[73] Such a posting can be analogized to a radio or television broadcast, which will be "to the public" even though no radio or television sets may be tuned to that channel at the specific time of the broadcast. It would appear, therefore, that all newsgroup postings would be considered to be communications to the public by telecommunication within the meaning of the *Copyright Act*. Similar considerations apply to messages posted to BBSs and on-line services such as America Online.[74]

Other Infringements

Even if the small number of recipients or the nature of an e-mail message means that the transmission of that message is not a communication "to the public", there may be other copyright infringements which occur as a result of the intermediate steps involved in getting the message from the sender to the recipients. Because the e-mail message will be

---

73 *Goldman v. The Queen*, *supra*.

74 In December 1996, a diplomatic conference under the auspices of the World Intellectual Property Organization (WIPO) agreed to two new treaties, the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. These two treaties will not come into force until 30 states join them and they will only be binding on those countries which actually join them. Nonetheless, they represent important international norms for the law of copyright and neighbouring rights.

Article 8 of the WIPO Copyright Treaty and Articles 10 and 14 of the WIPO Performances and Phonograms Treaty grant right holders rights with respect to the electronic communication of their works. Subject to certain limitations in the current Berne Convention, Article 8 of the WIPO Copyright Treaty grants authors of all works protected by copyright:

> "the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public or their works in such a way that members of the public may access these works from a place and at a time individually chosen by them."

The later part of this provision (ie. the "making available" right) is clearly intended to include Internet communications and other on-demand communications while excluding traditional "one-to-many" broadcasting. Because computer programs are considered as literary works and because they are explicitly covered by this treaty, they would be protected by this provision. Another important feature of this provision is that it grants the author the exclusive right to make the work available, and as a result no actual communication of the work is necessary to constitute an infringement. Posting a copyright work on a BBS, for example, would likely qualify as making the work available.

The two treaties and related documents may be found at the WIPO Web site at http://www.wipo.int.

saved on at least one mail server, there is a reproduction of the copyright work which infringes on the right granted in Section 3(1).[75] In addition, the viewing of an e-mail message or newsgroup posting by a recipient means that another reproduction has been made of the copyright work in the RAM of the recipient's computer.[76]

---

75 If the sender and recipient use the same ISP, the message may be reproduced only once. If they use different ISPs, the message will be reproduced at least twice.

76 This has been the position in the United States (*MAI Systems Corp. v. Peak Computer Inc.* (1993), 991 F. 2d 511; but see the contrary argument in respect of "browsing" in Loundy, "Revising the Copyright Law for Electronic Publishing", 14 J. of Comp. & Info. Law 1 (1995), at pp. 10-12) and England (*Intergraph Corp. v. Solid Systems Card Services Ltd.* (March 20, 1992, Ch. Div.) and *Digital Equipment Corp. v. LCE Computer Maintenance Ltd.*, summarized in (1992), 9 E.I.P.R. 184 (Ch. Div.)). A contrary result has been reached in Australia (*Autodesk Australia Pty. Ltd. v. Dyason* (1990), 18 I.P.R. 109 (Fed. Ct.), rev'd [1992] A.I.P.C. 90,855 (H.C.)) and Germany (*Nixdorf* v. *Nixdorf*, translated in [1991] 8 E.I.P.R. 301 (Ger. Fed. Sup. Ct.)). See Sookman, "Copyright and Technology", in Henderson, *Copyright Law in Canada* (1994), at pp. 299-300.

While it is by no means completely clear, it is expected that Canadian courts would follow the lead of the American and U.K. courts and hold that loading of a copyright image into RAM is in fact a reproduction.

Some of the difficulties involved in holding that the act of reading a copyright work by loading it into a computer would be an infringement of the reproduction right were noted by Guthrie, J. of the Quebec Superior Court in *Matrox Electronic Systems Ltd. v. Gaudreau*, [1993] R.J.Q. 2449:

> "A few historical comments may be helpful at this point. The recognition of copyright and the practice of paying royalties emerged with the printing press. The printing press was a bottleneck where copies could be examined and controlled. In the passage from the author's pen to the reader's hand, the press was the logical place to apply controls, be it to censor sacrilege or sedition or to protect the author's intellectual property. For modes of reproduction where such an easy locus of control as the printing press did not exist, the concept of copyright was not applied. For example, it was not applied to conversation, to speeches or to the singing of songs whether in private or in public.
>
> With the arrival of electronic reproduction and display, serious problems of adaptation have arisen. Electronic publishing is analogous not so much to the print shop of the eighteenth century as to word of mouth communication, to which copyright was never applied.
>
> Consider the crucial distinction in copyright law between reading and writing. To read a copyright text is no violation, only to copy it in writing. The technological basis for this distinction is reversed with a computer text. To read a text stored in electronic memory, one displays it on the screen, i.e. one writes it to read it. To transmit it to others, however, one does not write it; one only gives others a password to one's own computer memory. One must write to read, but not to write!"

The reproduction right is entirely separate from the other rights granted to the copyright owner. If the exercise of a right for which the defendant has a license also involves making a reproduction, and the defendant does not have a license to reproduce the work, then the defendant has infringed. This was demonstrated in the Supreme Court of Canada's decision in *Télé-Métropole Inc. v. Michel Bishop*.[77] The plaintiff Bishop was the composer of a musical work which was broadcast by the defendant television station. In order to permit future broadcasts, the defendant retained a tape copy of the performance of the work. No permission had been obtained for the making of a recording of the work, the rights to which were held by a mechanical rights collective.[78] The defendant argued that the broadcast license which it had obtained from the collective to which Bishop had assigned his performing rights included a license to make an "ephemeral" recording of the performance of the musical work to permit future broadcasts. The Supreme Court disagreed.

> "The right to perform (including radio broadcast), and the right to make a recording, are separately enumerated in s. 3(1) [of the *Copyright Act*]. They are distinct rights in theory and in practice."[79]

While some commentators have called for a "browsing" exception which would permit free access to view copyright material provided no permanent copy is made,[80] neither the present *Copyright Act* nor Bill C-32 provide such an exemption.

It has also been argued that such copying or retention of a copy of a copyright

---

77 [1990] 2 S.C.R. 467.

78 McLachlin, J. did not distinguish between the reproduction right and the recording right pursuant to Section 3(1)(d), and in fact uses the phrase "reproduction right" to refer to the right to make a record or other contrivance. In the context of that decision, this distinction probably was not material.

79 *Ibid*, at p. 477. It should be noted that McLachlin, J. based her recognition of the separate nature of these rights on the fact that, although both the public performance right and the recording right were subject to a form of compulsory license, they were based on different tariffs and administered separately. There would be even more of a distinction today as a result of the abolition of these compulsory licenses; see R.S.C. 1985, c. 10 (4th Supp.).

80 The basis for this argument is that copyright has traditionally not restricted the use to which copyright material could be used so long as additional copies are not produced. Just as there is no restriction on reading a book or viewing a videotape, it is argued, there should be no right to prohibit the perusal of a digital copy of a work: see Allard, "Copyright from Stone Age to the Celestial Jukebox", 17 Hastings Comm/Ent. L.J. 867 (1995), at pp. 8881-882 and Zimmerman, "Copyright in Cyberspace: Don't Throw Out the Public Interest with the Bath Water", *1994 Annual Survey of American Law* 403 at p. 407:

> "If browsing through works in a digital library is conceived of as an event that requires a copyright owner's permission, and if, furthermore, owners can prevent unconsented access directly by means of new technologies, then we could face a situation in which a user's intellect and imagination would be unable to engage someone else's intellectual property except through the mechanisms of cumbersome licenses and potentially onerous fee structures."

work should not be considered a separate copyright infringement if the making and keeping of such a copy is merely a technical step required for the facilitation of the Internet transmission which is itself the real use of the work. Some commentators have called for the creation of an "ephemeral exception" or a wider "caching exemption" by which copies of a copyright work could be freely reproduced as part of a system to transmit the works.[81]

Whether or not such an "caching exception" should be created in Canada is beyond the scope of this study. It is clear, however, that such an exception to the exclusive reproduction right is not recognized in the *Copyright Act* now in force, although potential infringements of copyright or the performers' right are currently subject to certain exceptions for temporary fixations made for the purpose of review or permanent fixations made for archival or legal disclosure purposes.[82] Bill C-32 has not proposed implementing such an exception,[83] and, in view of the decision of the Supreme Court of Canada in the *Télé-Métropole* case, it is difficult to see how such an exception could be recognized in Canada without a specific legislative amendment. Such an amendment might also be a breach of Canada's obligation as a signatory to the Berne Convention.[84]

A problem may also arise where portions of the new work are stored in multiple locations and only assembled when the work is accessed. The *Copyright Act* only prohibits the reproduction of a "substantial part" of a copyright work. If a copyright work is divided into many parts in such a way that each part is not a "substantial part" of the entire work, then it could be argued that the reproduction of each of these parts is not an infringement; there could of course be an infringement if the parts were re-assembled into the entire work. This concept has a number of ramifications. First, it offers a potential way for infringers to avoid liability for infringement of the reproduction right by ensuring that they do not store more than a small portion of a work in any one place. It must be noted that it would be difficult, if not impossible, to identify a fragment of a work on a storage device or determine whether that fragment is a substantial part of the work. Second, it is at least theoretically possible to store the fragments of a work in different countries so that it cannot

---

81 See Schlacter, "Caching on the Internet", 1-7 *Cyberspace Lawyer* 2 (1996). The opposing argument is that caching interferes with the copyright owner's control over its works, prevents timely updating of cached pages and distorts the counting of the number of "hits" to a Web page, which can be an important factor in attracting advertisers to commercial sites. Caching is also discussed in the next section of this report.

82 See Sections 28.02(2) and 27(2)(h), (i), (j) and (k) of the *Copyright Act*. Bill C-32 will extend these same exemptions to copyrights in sound recordings.

83 The IHAC Copyright SubCommittee recommended against creation of an ephemeral exception, and concluded that browsing was a reproduction: IHAC Copyright Report, pp. 14-15. The IHAC Report recommended (recommendation 6.4) that while browsing should be defined in the *Copyright Act*, it should be left to the copyright owner to determine whether and when browsing should be permitted.

84 There is a limited right in Article 9(2) of the Berne Convention to pass domestic legislation to permit the reproduction of works in "certain special cases", provided that "such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author". It is unclear whether a general "caching exception" could meet the threshold established by Article 9(2).

be argued that the totality of the activity in any country is an infringement.

If an e-mail communication is not "to the public" so as to constitute an infringement of the exclusive telecommunication right granted in Section 3(1)(f), then the exception contained in Section 4(1)(f) (which provides that a communication to the public is not a publication) also does not apply. As a result, if a "private" e-mail communication contains an unpublished copyright work, the sending of the work by e-mail may be the "making of copies available to the public" so as to constitute publication of the work.[85]

Lastly, even if the communication of an unauthorized copyright work is not "to the public", it may be an indirect infringement if the requirements of Section 27(4) are satisfied. In particular, an e-mail message to a single recipient could be a sale or offer to sell the work, a distribution of the work, either for the purposes of trade or which prejudicially affects the copyright owner,[86] or an importation into Canada for sale.[87] In each case, the sender of the e-mail would have to be aware that the work infringes copyright.

In summary, it would be appear that, without exception, every e-mail and

---

85 It is possible that an e-mail message can be both the making of copies "available to the public" and not a "communication to the public" since the former requires a direct communication while the latter would seem to refer only to the potential that copies will actually reach the public.

It was likely the original intention of the *Copyright Act* that the concept of publication be limited to portable physical copies of the work. For example, Section 5(c) requires that a first publication be "in such a quantity as to satisfy the reasonable demands of the public"; such a provision makes little sense if "publication" includes digital transmission of copies since just one initial copy of a work can very quickly be disseminated around the world on the Internet. Because the definition of publication does not specify that it is limited to physical copies, however, it is possible that a court could interpret this section as applying to digital copies as well in the very narrow circumstances set out above.

It appears that in England the distribution right is limited to "physical copies" of works, and services which provide digital copies of musical works do not distribute the works: see John, "What Rights Do Record Companies Have on the Information Superhighway?", [1996] 2 E.I.P.R. 74, at p. 76.

86 In *Playboy Enterprises, Inc. v. Frena* (1993), 839 F. Supp. 1552 (Fla.), the Court found that the posting of copyright photographs to a BBS was an infringement by the BBS sysop of the U.S. public distribution right. The analysis in this decision has been widely criticized (see Elkin-Koren, "Copyright Law and Social Dialogue on the Information Superhighway", 13 Cardozo Arts and Entertainment L.J. 346 (1995) and Loundy, "Revising the Copyright Law for Electronic Publishing", 14 J. of Comp. & Info. Law 1 (1995)) and was rejected by Justice Whyte in the *Netcom* decision, at pp. 12-13. It is unlikely that the same result would obtain in Canada since the sysop denied any knowledge of the infringing postings, and knowledge is an essential element of indirect infringement pursuant to Section 27(4).

87 It is unlikely that the importation prohibition in Section 27(4)(d) and the detailed importation provisions contained in Sections 44, 44.1 and 45 apply to digital copies of works in addition to physical copies of works. The IHAC Copyright SubCommittee was of the view that "electronic importation is not possible" since the original of the work is not imported; rather, a new copy is made in Canada when the work is downloaded by a recipient or uploaded to a server or BBS located in Canada: see IHAC Copyright Report, p. 12. This approach appears to be in accord with a purposive reading of the *Copyright Act*, but there is no Canadian case law which is of assistance.

newsgroup message which contains or attaches copyright material for which no appropriate authorization has been obtained from the copyright owner infringes the exclusive reproduction right of the copyright owner. In addition, all newsgroup postings, and many e-mail messages, may constitute a communication of the copyright work to the public by telecommunication, depending on whether the posting or message is considered to be "to the public". Even if some e-mail messages are considered to be "private", they may involve a publication of the work if it was previously unpublished. Lastly, if the infringer has the requisite knowledge, the sending of e-mail and newsgroup messages may constitute indirect infringement pursuant to Section 27(4).

(ii) World Wide Web, FTP Sites and BBSs

The nature of World Wide Web, FTP and BBS access is somewhat different from e-mail and newsgroup postings. While initially data must be made available on a Web page, FTP site or BBS, to a large extent it is the recipient which originates and controls access to, and downloading of, the data to be retrieved.

The first step is the making of data available to be downloaded. A Web page[88] owner will place the elements of the page on a server with a certain identifying address. Users who wish to access the page, or some element of it, instruct their Web browser software to locate the elements of the page where they are stored on a server. The browser software then retrieves and downloads these elements through the Internet (and the user's ISP, if applicable) to the user's computer. The elements of the Web page are then interpreted by the user's Web browser and displayed on the computer screen.

The elements of a Web page may be text, graphics, sound or video. Increasingly sophisticated Web browsers are permitting more varied elements to be incorporated in Web pages. It is expected that, as transmission bandwidth improves and user computers become more powerful, Web pages will eventually allow real time reception of video signals which will rival those of television transmissions.[89] Each Web "broadcast" can only be made to a finite group of receivers. The Web page's host server must handle each request for access individually and may not be able to keep up with demand at any specific time. Access to a Web server, no matter how many access lines are added, is a true bottleneck which has no equivalent in conventional "one-to-many" broadcasting.

---

88 The term "page" is used, somewhat inaccurately, to refer to an individual URL address.

89 Live radio broadcasts are already common on the web. As of November 24, 1996, the MIT radio site lists 170 radio stations worldwide (including six in Canada) which provide live Internet access to "bitcasts" of their signal: see http://wmbr.mit.edu/stations/list.html. Internet television broadcasts have been tried in the United States but thus far have been abandoned, probably due to a combination of technical unavailability of adequate bandwidth and questions concerning regulation of such transmissions as "broadcasting". There does appear to be one "time-delayed" live television broadcast from Sweden's SuperSport channel: see http://www.filmnet.see/playing now/playing now.html.

The second step is under the control of the user who must access the information in the Web page, FTP site or BBS. Very often the user initiating a download from an FTP site or BBS will not know exactly what it is that is being accessed as a result of the use of cryptic or ambiguous file names. This is sometimes true on the Web as well when a page is first accessed through a link from another page, but the user who accesses an individual element on a page (such as a link to a graphic or a sound) will generally have an idea of what will be downloaded.[90] Web users who wish to access the page, or some element of it, instruct their Web browser software to locate the elements of the page where they are stored on a server. The browser software then retrieves and downloads these elements through the Internet (and the user's ISP, if applicable) to the user's computer. The elements of the Web page are then interpreted by the user's Web browser and displayed on the computer screen.

One unique element of the Web which is critical to the issue of copyright liability is the act of "caching". Unlike e-mail communications, the basic transmission of the elements of a Web page from the server in which they reside to the recipient's computer is "instantaneous" and need not involve a reproduction of the work by the ISP of the recipient. To that extent there may be less reproduction of copyrighted works in Web page access than in e-mail communication. Caching, however, involves the storage of the elements of a Web page on an intermediate server or computer so as to increase the efficiency of accessing that page. Caching is done by both ISP's and users.

ISP's cache heavily-accessed pages in order to speed the access time experienced by their users and minimize network logjams. This is especially important for access to overseas Web sites which can result in significant communication delays. By caching popular overseas sites, ISPs can reduce the extent of these delays. Caching by ISPs can be either "blind" (ie. done by operation of their system automatically based on demand or technical requirements) or based on specific choices made by the ISP for technical or commercial reasons.

Users also cache Web page elements, although usually not advertently. All of the popular Web browsers make extensive use of "blind" caching, again to improve efficiency. The elements of a Web page are stored on a user's hard drive when a page is first accessed in a Web session, and, depending on the Web browser's options, the cached copy of the Web page's elements will often be accessed later without recourse to the Internet or a new download. In most cases, user caching will take place without any active intervention or choice on the part of the user. Often, depending on the Web browser and how it is configured, a user may be saving the contents of hundreds of Web pages on their hard drive without the user knowing that this has been done.

---

90 This raises the interesting question of the potential liability of the user which deliberately or negligently mislabels a file which is then downloaded by another user in reliance on the misdescription of the file's contents: Hardy, "The Proper Legal Regime for 'Cyberspace'", 55 U. of Pitt. L. Rev. 995 (1994), at pp. 1014-1015.

It is also relevant to note that, unlike a television signal, a Web page's elements may produce radically different images or sounds for different users, depending on the Web browser being employed and the ancillary software which the user employs. The images or sounds generated for each user are an interpretation of the elements placed in the Web page by its creator.[91]

As in the case of e-mail and newsgroup postings, it will be apparent that the accessing of a Web page containing unauthorized copyright material may infringe that copyright in a number of ways. The initial placement of unauthorized copyright material onto the Web page, FTP site or BBS will be an infringement of the reproduction right and, just as with e-mail communications, could be infringement of other rights. What is less clear is whether the transmission and downloading of such material is an infringement as well.

The posting of a copyright work to a BBS which permits users to download material to the BBS for future retrieval by other recipients would clearly be a reproduction of the work. In addition, employing the same logic which would apply to a "broadcast" e-mail, it is likely such a posting would also constitute a communication to the public by telecommunication, even if no user subsequently downloaded the work from the BBS, since the intent of the posting is to communicate with an unknown number of users who may not be known to the poster.

The communication of a copyright work from a Web site to the user would appear to be a communication ″to the public″ by telecommunication. The private/public distinction discussed above in relation to e-mail communication has no application to Web sites which are freely accessible by any Internet Web user[92] since the intention of creating the Web page is to allow unidentified users to gain access.

---

91 This fact has been put to good use by some Web page designers, who are starting to use information about the user to determine which advertising or other message should be included in the image sent to the user's computers. It is expected that Internet communications will become even more specialized to the individual user in the future.

This flexibility raises vexing copyright issues. For example, if a Web page contains an unauthorized copy of a copyright graphic image, but the user downloading the page is using a text-only browser, is there a communication of the work? The poster intended to send it, the binary signal sent to the recipient contains the information necessary to view the copyright work, but the recipient does not have the ability (or inclination) to view it. The recipient may have unwittingly reproduced the work in their computer's storage (if the page is cached), but it is difficult to see that a "communication" of the work has occurred. See Loundy, "Revising the Copyright Law for Electronic Publishing", 14 J. of Comp. & Info. Law 1 (1995), at pp. 27-28.

92 Note that it is unclear whether the same considerations would apply to communications over "Intranets", which might be private and exclusive to a very small group of individuals. Although such Intranets are beyond the scope of this study, it should be noted that the copying of video cassette tapes solely for "private" use within a company has nevertheless been found to be an infringement of the reproduction right: *Tom Hopkins International Inc. v. Wall & Redekop Realty Ltd.* (1984), 1 C.P.R. (3d) 348 (B.C.S.C.); aff'd on this point (1985), 6 C.P.R (3d) 475 (C.A.).

To the extent that the Web page's elements are cached by the user's ISP, this caching will constitute a reproduction of the copyright work. Many ISPs and telecommunications carriers see the need for some type of "caching exemption" which would permit the reproduction and storage of copyright works solely for the purpose of increasing communication efficiency. They argue, with some justification, that it is in the interests of all stakeholders, including copyright owners, that Internet efficiency be maintained so that the value of the communication can be maximized, and that it is unfair that ISPs should be potentially liable for an unknown, but significant, number of technical copyright infringements over which they have little control. Copyright content owners, on the other hand, say that the ISPs are making use of the copyright works in a way which benefits the ISPs and their users but produces no value for the copyright owners.

As noted above, whatever may be the advantages or disadvantages of permitting such a "caching exemption",[93] it is clear that neither the current *Copyright Act* nor Bill C-32 would permit the free reproduction of copyright works for the purpose of caching.[94]

Because of the hyperlinked nature of the Web, there is increasing controversy about the propriety of a Web page owner including "unauthorized" links to other Web pages. For example, the owner of copyright images might decide to place an electronic copy of those images on the Web as a promotional tool. The owner might design an intricate series of Web pages which are intended to encourage users to purchase the owner's other products. Each of the copyright images placed on the Web by their owner are situated in individual Web pages which are accessed by links from various other pages created by the copyright owner in such a manner as to project a certain image. While it is clearly the intention of their

---

93 The policy considerations which are involved in considering such a exception are numerous and complex. Some obvious ones include:

(a) What protection would be available to ensure that "cached" copies held by ISPs would not be publicly available? This is of great concern because many ISPs are very small operations which cannot afford elaborate security measures.

(b) There may be commercial disadvantages to a copyright owner if Web pages containing their works are cached, particularly if compensation to the copyright owner is based on the number of "hits" to the Web page containing the copyright works. Because the caching by an ISP involves only one hit to the Web page, but may in fact result in many more accesses by individual users, the copyright owner may have the use of their works significantly devalued. The potential for "targeted" advertising messages is also reduced if a Web page is cached by an ISP since there is less opportunity to communicate with the user directly.

(c) There could be significant international trade issues involved. If ISP liability due to caching becomes excessive, Canada may lose ISPs to other countries which do not impose such restrictions, provided that the additional cost of moving off-shore (including telephone connections) is less than the royalties or damages payable to copyright owners. Alternatively, if ISP liability is clarified in Canada at a level which is considered to be reasonable, this could encourage ISPs to locate in Canada.

94 There is, however, an issue concerning who is liable for caching infringements; see the discussion of "Liability of Intermediaries" below.

copyright owner that the Web pages containing the copyright images only be accessed through the owner's other pages, there is no mechanism on the Internet to prevent another Web page creator from including an unauthorized link to the pages containing the copyright works. In fact, the Web page making the unauthorized link may even be owned by a rival of the copyright owner and the links to the copyright works may be used to denigrate or criticize the works.

Although the copyright owner may not like the links being made by a third party to the location of its copyright works, it is difficult to see how there is any infringement of the copyright in the works to which the links point.[95] The linking Web page is no different from a footnote or bibliography which points a user to another location or source. The only information which is contained in the linking Web page is the URL of the linked page, and, just as there can be no copyright in the title of a book, play or music,[96] there likely can be no copyright in a URL address itself.[97]

There has recently been a strange case in Scotland involving an ongoing dispute between *The Shetland Times* and *The Shetland News*.[98] Both the *News* and the *Times* have Web sites. The *Times* site contains headlines which link to various news stories. In October 1996, the *News* began to place headlines on its Web site. Each of the headlines on the *News* Web site linked to a news story in the same way that the *Times* Web site did, but the *News* copied some of the headlines used by the *Times* and used them to link directly to the corresponding stories on the *Times* Web page. On October 24, 1996, the *Times* obtained an interlocutory injunction from Lord Hamilton prohibiting the *News* from using the headlines to link to the stories on the Times Web site. The decision has received widespread publicity and has been decried by many Internet participants.

In fact, Lord Hamilton's decision is a limited one which should have little application to Canadian copyright law. In granting the injunction to prevent the linking by the *News*, Lord Hamilton applied a standard two-part test. The first part of the test is to

---

95 This analysis is not limited to copyright images contained on Web pages, since each Web page in itself is a copyright work which is owned by its creator.

96 "Copyright does not extend to a single word, name or title as that is the field of trade marks, not copyright.": *Hughes on Copyright and Industrial Design* (1984) at p. 355-4 and *British Columbia v. Mihaljevic* (1989), 26 C.P.R. (3d) 184, 190; aff'd (1991), 36 C.P.R. (3d) 445 (B.C.C.A.). There is some authority that the copying of the title of a work could be an infringement of copyright if the title is itself a "substantial part" of the work: *Frances Day & Hunter Ltd. v. Twentieth Century Fox Corporation*, [1940] A.C. 112 (P.C.).

97 In his submission to this study, Marc Plumb notes that, from a policy point of view, it might be inadvisable to limit the ability of a Web page to point to another Web page since that would possibly prevent many desirable reference such as the anti-hate pages which link to pages placed by hate groups and refute their claims. Such links might be impossible if the owner of the hate page could prevent them as an infringement of copyright.

98 Lord Hamilton's reasons for granting the interlocutory injunction have recently been made available on Quicklaw in Canada and LEXIS/NEXIS. Details of the dispute can be obtained at http://www.shetland.news.co.uk/appeal.html.

determine whether there is an arguable case put forward by the plaintiff. The *Times* argued that there was copyright in the headlines which were copied by the *News* and that the headlines were "cable programmes" within the meaning of section 7 of the U.K. *Copyright, Designs and Patents Act, 1988*. Lord Hamilton admitted that no technical information about how the Internet worked had been put before him, and he decided that it was at least arguable that the *Times* Web site fell within the definition of "cable programme". The decision can therefore be seen as simply a narrow and very preliminary interpretation of section 7 of the U.K. statute, and there is little in the judgment that sets out general principles concerning Internet liability. On the issue of whether there is copyright in the headlines themselves, the solicitor for the *News* admitted that it was possible in some circumstances that headlines could in themselves be literary works subject to copyright, and it was therefore easy for Lord Hamilton to conclude that the *Times* had at least an arguable case.

The second part of the interlocutory injunction test is to determine where the balance of convenience lies. Lord Hamilton decided that since the *News* had only recently started to refer to the *Times* headlines, there would be no prejudice to the *News* if it was prohibited from continuing the practice until trial of the issue. Lord Hamilton's decision does not deal with the more general issue of whether a Web page owner can prevent another person from linking to his or her site, and there is nothing in the judgment which would lead to the conclusion that there is any such restriction.[99] Further clarification of this decision and potential limitations on the right to link to Web sites will have to await future court decisions or possibly legislation.

Although a link itself likely cannot be copyrighted, there may be copyright in a compilation or collection of links, depending on if the compilation meets the originality test for copyright protection.[100]

FTP sites and BBSs can take a number of forms, but a common characteristic is that, like Web pages, communications are driven by the user which seeks access to the information stored in the FTP site or BBS.[101] Access to most FTP sites or BBSs do not involve caching activities. If an ISP is involved, there is normally no retention on the ISP's server of any of the data which is downloaded by the recipient.

If the communication from the FTP site or BBS contains a copyright work, then the

---

99 The *News* could have avoided altogether the issues raised by the *Times* by creating new headlines to use as links to the stories on the *Times* Web site. Although this solution would likely avoid any question of copyright infringement, the *Times* could claim passing off or some similar tort if the *News* did not make it clear that the articles being linked to belonged to the *Times* and not the *News*.

100 Georgini, "Through Seamless Webs and Forking Paths: Safeguarding Author's Rights in Hypertext", 60 Brooklyn L. Rev. 1175 (1994), at pp. 1195-1196.

101 Included in the widest definition of "BBS" would be on-line services such as America Online and Compuserve. A large portion of the value which these services provide consists of collecting in an organized fashion digital information which can be accessed by users.

download by the recipient is a reproduction of the work. This is the case even when the work is only "browsed" since the work is nevertheless reproduced in the RAM of the recipient's computer.[102]

Further, most, if not all, downloads of copyright works from FTP sites or BBSs will also constitute communications to the public by telecommunication. Because the nature of FTP sites or BBSs are such that they invite a number of unrelated persons to access them in order to facilitate communications which presumably could not take place solely through private e-mail, it is unlikely that such communications could reasonably be seen as private and not "to the public".

Lastly, it is unlikely that an Internet transmission could ever be found to be a public performance. If the transmission is a communication to the public by telecommunication, then, as a result of Section 3(4), the transmission cannot also be a public performance. If the transmission is not "to the public" (because it is private e-mail, for example), then, while Section 3(4) does not apply, the transmission also would not be a "performance in public" as required by Section 3(1). The case law has indicated that the phrase "to the public" is of wider import than the phrase "in public".[103]

(iii) Conclusion

In summary, the following exclusive rights appear to be likely to be infringed on the Internet when an unauthorized transmission of a copyright work is made:

(a) virtually all communications of copyright works on the Internet, even those contained in "private" e-mail, involve a reproduction of the work within the meaning of Section 3(1)(a) of the *Copyright Act*;

(b) some unauthorized e-mail communications of literary, dramatic, musical or artistic works on the Internet will infringe the right to communicate to the public by telecommunication within the meaning of Section 3(1)(f) of the *Copyright Act*. Whether a particular e-mail message is an infringement will depend on the number of recipients of a communication and the purpose and methodology employed by, and possibly the intent of, the sender of the communication;

(c) all unauthorized communications of copyright works which involve "on-demand" access (such as BBSs and Web sites) infringe the right to communicate "to the public";

---

102 See discussion at footnote 76.

103 *CCTA*, at p. 367; *CTV*, at p. 354.

(d) In the case of "private" e-mail by which the copyright work is not "communicated to the public" but is considered, as a result of the e-mail communication, to have been made "available to the public", there may have been a "publication" within the meaning of Section 4(1) of the *Copyright Act*, provided that (a) the communication does not meet the requirements for being a communication to the public by telecommunication under Section 3(1)(f), and (b) the work is previously unpublished;

(e) if the infringer has the requisite level of knowledge, a distribution of an unauthorized copy of the copyright work over the Internet could be an indirect infringement pursuant to Section 27(4).

It should be noted that Internet transmissions containing literary, dramatic, musical or artistic works are not performances of the works in public.

(b) Where Does Internet Copyright Infringement Take Place?

The next step in identifying where liability for copyright infringement on the Internet might lie is to analyze where the infringement might take place.

The international nature of the Internet has led to jurisdictional issues which have only rarely been considered in Canadian copyright law. Initially, copyright law dealt only with tangible works such as books, phonograph records (and improvements such as CDs) and later motion pictures (and refinements such as video tapes). Because the copying of a tangible work must take place in one location, it is relatively clear where copyright has been infringed if unauthorized copying takes place.[104] Further restrictions on unauthorized copies are imposed by import controls.[105]

The Internet raises difficult jurisdictional and conflicts of laws questions due to its international reach and multi-nodal nature. A user in Canada can dial into an ISP in another country and access a Web site anywhere in the world. The communication of the Web site elements to the user in Canada over the Internet could route through several countries in addition to the country where the ISP is located and the location of the Web site server. One author recently described the problem in this way:

---

104 In *Compo Co. Ltd. v. Blue Crest Music Inc.*, [1980] 1 S.C.R. 357, the Supreme Court of Canada referred to, but did not specifically adopt, a series of cases in the United States, starting with *G. Ricordi & Co. Inc. v. Columbia Graphophone Co.* (1920), 270 F. 822 , which held that preliminary steps in the production of a record could amount to "manufacturing" under the United States *Copyright Code* even though the final product was pressed in Canada. There does not seem to be any question that significant activity leading to the manufacture of the infringing article is required in the country in which it is alleged the infringement took place.

105 Sections 27(4)(d) and 28.02(3)(d).

> "To understand the question of jurisdiction, consider this situation: A programmer in France accesses a computer system in Kuwait, via intermediary computers in the United States, and makes a copy of a computer program, the rights to which are owned by an American software company, and places that software on a computer in Guatemala.
>
> Has copyright infringement occurred? If so, in which jurisdiction? Neither Kuwait nor Guatemala appear to be signatories to any of the major copyright conventions such as Berne or the Universal Copyright Convention.
>
> The passage of the apparently illicit copy of the software through the U.S. was fleeting - perhaps to the point that at any given moment in time no more than 512 characters of information were resident in the U.S. The apparently illicit copy, once made, comes to rest in Guatemala.[106]

These concerns are not at all theoretical. In a recent paper,[107] Professor Geller posits the following example:

> Suppose that, without any right-holders' consent, a media enterprise headquartered in the United States colorizes Buster Keaton's classic film work *The General* and makes this version accessible in digital format through a trans-Atlantic network. End-users in France and Germany can order the work through the network, while the enterprise is paid through credit-card accounts for providing this access. In the United States, copyright in this work has lapsed; in France, moral rights protect it, but not economic rights; in Germany, all rights in it still subsist.[108]

---

106 Johnson-Laird, "Legislating the Internet: Is It Already Too Late?", 1-6 *Cyberspace Lawyer* 12, at p. 13 (1996).

107 Geller, "Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Network World", 20 Columbia-VLA Journal of Law & The Arts 571 (1996).

108 Geller, *supra*, at p. 571. Compare the Judgment of April 24, 1974 (French Keaton decision), Cour d'appel, 1re (Paris), 83 REV. INT'L DU DROIT D'AUTEUR (RIDA) 106 (1975), English trans. in 7 I.I.C. 130 (1976), aff'd, Judgment of December 15 1975, Cass. civ. 1re, 88 RIDA 115 (1976) (lapse of copyright in the United States results in expiry of economic rights in France) with the Judgment of January 27 1978 (German Keaton decision), Bundesgerichtshof, 1979 GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT - INTERNATIONALER TEIL (GRUR INT.) 50; English trans. in 10 I.I.C. 358 (1979) (Keaton's works are still protected in Germany). It appears that, under French law, moral rights are perpetual: see CODE DE LA PROPRIETE INTELLECTUELLE art. L. 121-1 (1992).

These types of examples raise two main issues. First, what law is to be applied in determining whether copyright subsists in the works which are alleged to have been infringed? This is a conflict of laws issue which has been debated for some time in respect of satellite communications, with little international or national consensus on what the legal answer should be.[109] If the law of the receiving country is to be applied to determine whether copyright exists in the work and has been infringed by the communication, then communications of works which are not infringing in the transmitting state could result in an infringement in the receiving state, even if the transmission was not intended to reach that state. Alternatively, if the laws of the transmitting state determine these issues, this creates a risk of forum shopping in order to locate the "least protective country" from which copyright infringers could then act with impunity. The resolution of this issue is beyond the scope of this study.

The second issue is a jurisdictional one. In the absence of international agreements to the contrary, a copyright is strictly territorial in its application, and no action lies in Canada for either an infringement of a Canadian copyright which takes place beyond Canada's borders[110] or an infringement in Canada of a copyright granted pursuant to the law of a foreign country.[111] "The protection given under the [Canadian Copyright] Act is territorial and generally speaking there is no jurisdiction to prevent infringement outside Canada".[112]

---

109 See Geller, *supra*, at p. 572.

110 This issue was considered in *Tele-Direct (Publications) Inc. vs. American Business Information Inc.* (1996), 113 F.T.R. 123, 27 B.L.R. (2d) 1 (F.C.T.D.). The defendant ABI offered a database access service over the Internet from its main office in Nebraska. There was a dispute concerning whether the availability of copyright material in an American database which was available to be accessed by Canadian subscribers could be copyright infringement in Canada. As a result of the Court's decision that the ABI database and publications did not infringe Tele-Direct's copyright, the Internet issue was not dealt with.

111 A Canadian copyright is generally granted to foreign works by Section 5 of the *Copyright Act*. A work is considered to have Canadian copyright if:

a) at the time the work was made, the author was a British citizen, a citizen, subject or resident of a "treaty country" or a resident "within Her Majesty's Realms and Territories";

b) at the time a cinematograph is made, its maker satisfies the above tests or, if the maker is a corporation, had its headquarters in a "treaty country";

c) in the case of a published work, it is either published first in a "treaty country" or "within Her Majesty's Realms and Territories" or, if first published elsewhere, is published within 30 days in a "treaty country" or "within Her Majesty's Realms and Territories".

Section 5 creates a Canadian copyright for most foreign works, but does not extend the ambit of the *Copyright Act* to enforce foreign copyrights. As a result, any right granted by the domestic law of another state, even another treaty country, will ccnot be enforced by Canadian courts, although an equivalent right may exist under Canadian Law.

112 The Canadian Encyclopedic Digest (Ontario) (3d ed.), Vol. 5, "Copyright" at ¤13; Dicey & Morris, "The Conflict of Laws" (12th ed., 1994), at p. 1516; *Def Lepp Music v. Stuart-Brown*, [1986] R.P.C. 273 (Ch. Div.). The position in the United States on jurisdiction over copyright infringements occurring abroad

Infringements outside Canada must be dealt with pursuant to the copyright legislation in which the infringement takes place.

To date, Canadian copyright jurisprudence has been surprisingly inconclusive in its treatment of wireless or electromagnetic communication of copyright works from outside of Canada and it has never been determined whether a broadcaster outside of Canada can infringe copyright in Canada when its signal crosses the Canadian border. In *Composers Authors and Publishers Association of Canada v. International Good Music, Inc.*,[113] the Supreme Court of Canada dealt with an application to set aside service of a statement of claim in the United States. The defendants were alleged to have broadcast copyright music into Canada from a television transmitter located just south of the border with British Columbia. The defendants did not have a license to publicly perform the music in Canada. After noting that there was no Canadian case law on point, the Supreme Court held, based on *Jenner v. Sun Oil Co. Ltd.*,[114] that there was a "good arguable case" that the defendants were communicating in Canada the musical works in question. There is no reported resolution of this issue in subsequent proceedings.

The decision of the Supreme Court in the *International Good Music* case seems to be based on a tort analogy in that the Court referred to *Jenner v. Sun Oil Co. Ltd.*, a defamation case. It has since been held by the Supreme Court that tort law does not apply to copyright infringement claims in Canada.[115] Early commentary on the *International Good Music* case noted that the Supreme Court explicitly did not decide the copyright infringement issue,[116] but more recent articles seem to have accepted that the lack of case law since the Supreme Court's decision implies that broadcasting from outside Canada may be a violation of Canadian copyright.[117]

---

is unclear: see Cinque, "Making Cyberspace Safe for Copyright", 18 Fordham Int. L.J. 1258 (1995), at pp. 1279-1285.

The other potential issue is whether a Canadian court would have personal jurisdiction over a person outside of Canada in these circumstances. In *Compuserve v. Patterson* (1996), 89 F. (3d) 1257 (6th Circ.), it was held that an action could be commenced by Compuserve in Ohio against a Texas resident who had posted shareware to one of Compuserve's forums. The court found that Patterson had marketed his product in Ohio by dealing with Compuserve, which he knew had its main computer facility in Ohio. See also *California Software, Inc. v Reliability Research, Inc.* (1986) 631 F. Supp 1356 (Cal.). Canadian courts have taken a very wide view of the scope of personal jurisdiction, subject only to consideration of *forum non conveniens*.

113 [1963] S.C.R. 136.

114 [1952] O.R. 240.

115 *Compo Co. v. Blue Crest Music Inc.*, [1980] 1 S.C.R. 357 at 372.

116 Fox, *The Canadian Law of Copyright and Industrial Design* (2nd ed., 1967), pp. 404-405.

117 Nesgos, "Canadian Copyright Law and Satellite Transmissions", 20 Osgoode Hall Law Journal 232 (1982), at pp. 240-241.

It is possible that there could be a distinction between intentional and incidental cross-border broadcasting. In particular, Martland, J. stated in *International Good Music*:

> "The issue which would have to be determined in the present case, if it is tried, is as to whether a person who operates a television transmitter outside Canada, **but with the primary object of transmitting programmes for reception in Canada**, can be held to have communicated a musical work by radio communication in Canada, so as to have infringed the rights of the holder of the Canadian copyright in such work. ...
>
> To me it seems arguable that a person who has held himself out to advertisers as being able to communicate, by means of his American television transmitter, with some 1,000,000 persons in British Columbia, if he transmits musical works, of which the appellant [collective] has the Canadian copyright, to viewers in Canada who receive such programmes, has thereby communicated in Canada such musical works by radio communication.[118] (emphasis added)

This is an indication, although far from a conclusive one, that a signal which is intended to reach Canadian recipients could be a copyright infringement in Canada, while a signal which is intended for a foreign audience but incidentally reaches Canada might not be.

The application of these principles to determine the location of individual types of copyright infringement on the Internet ranges from relatively simple to very difficult.

The easiest analysis relates to infringements of the reproduction right. Reproduction is an integral part of virtually every Internet communication which contains copyright works. In most Internet communications containing copyright works, a reproduction is done initially by the sender or poster (when they place a copy of the work on their computer or server) and again by the recipient when downloading the work from wherever it is stored. In addition, intermediaries such as ISPs routinely make reproductions of works. Some of the reproduction may be "blind" (such as the caching of Web pages and the retention of e-mail messages on mail servers) and some will be advertent and intentional

---

118 *International Good Music*, *supra*, at pp. 143-144.

(such as when an ISP provides an FTP site of software for use by its customers).

An Internet infringement of the reproduction right takes place at the location of the storage device on which the unauthorized copy of the work is made. It is the actual recording of the electromagnetic impulses representing the work which constitutes a reproduction. Therefore, a reproduction of a copyright work could take place in the country where the recipient of an e-mail, a newsgroup server or an ISP's server is located. This is true even if the sender of the message is located in another country. Since almost all Internet communications involve a reproduction, this makes locating the country of many copyright infringements relatively simple, provided that the recipient computer can be located.

The determination of the location of a communication by telecommunication is more difficult. An infringement of the right to communicate a work to the public by telecommunication could be seen to take place in any one or more of:

a) the country of the sender[119]

b) the country where the sender intended the message to go (even if it ended up somewhere else)

c) the country of any recipient

d) any country through which the transmission passes in being delivered

e) in the primary location of the ISP of either the sender or the recipient.[120]

Such an analysis can become even more complex when portions of an Internet message are located in several different countries or if there are multiple recipients.

Because the *Copyright Act* uses the phrase "to the public" in referring to communication by telecommunication, it strongly implies that it is the location of the recipient which is critical. This seems to have been the conclusion arising from the earlier case law relating to public performances:

---

119 The European Union's Satellite Directive employs the law of the country of "uplink" to determine liability for the broadcast of programming by satellite: see Council Directive 93/83/EEC, [1993] O.J. L248, preamble 14, Article 1(2)(b), in Skone James, *Copinger and Skone James on Copyright* (1st Supp., 1995), pp. 415-425.

120 See Ginsburg, "Putting Cars on the "Information Superhighway": Authors, Exploiters and Copyright in Cyberspace", 95 Columbia L. Rev. 1466 (1995), at pp. 1496-1498 for a discussion of this issue under United States law.

> "Who then is liable [when a radio broadcast is made from the United States to Canada without permission from the Canadian copyright owner]? Not the person or persons responsible for the broadcast in the United States because they own the copyright therein and are only doing what they have every right to do. They cannot control the passage of the electrical impulses over the ether across the Canadian border. Obviously, therefore, the infringer (if any) is the person operating the radio receiving set in Canada, and if the radio receiving set operates in public, a performance thereon of works in which copyright subsists in Canada will, in the absence of license or consent, constitute infringement."[121]

The various broadcast tariffs approved by the Copyright Board in respect of such communications of musical works to the public are currently addressed only at Canadian broadcasters and cable operators despite the fact that transmissions originating in the United States reach Canadians.[122] Only in the event of the retransmission to recipients in Canada of

---

121 Fox, *The Canadian Law of Copyright and Industrial Designs*, (2nd ed., 1967), at p. 403. This opinion was based on the decision of Viscount Maugham in *Mellor v. Australian Broadcasting Commission*, [1940] 2 All.E.R. 20 (P.C.). It is important to note that the recipient would not be performing the work in public simply by receiving or viewing it. The work would have to be disseminated further to the public.

United States v. Thomas, 1996 Fed.App 0032P (6th Cir., 1996)(available at http://gopher.eff.org/pub/Alerts/us_v_thomas_appeal.decision) dealt with a California BBS sysop who was convicted of distributing obscene material in Tennessee when a Memphis resident (an undercover agent) downloaded sexually explicit material from the BBS. It was not contested that Thomas would not have been convicted in California since the material in question did not violate "community standards" in that state. While the result would seem to support the idea that the relevant location for liability is that of the recipient, the actual decision is rather sparse on the jurisdictional question.

122 See, in particular, Tariffs 1 and 2. Radio and television stations located in the United States are routinely received in Canada but pay no royalties in Canada for the use of music or other copyright material contained in their programs. Canadian retransmitters of these border signals pay retransmission royalties for conveying these signals to Canadians through cable systems, but it is clear that the retransmission activity takes place in Canada: see Section 28.01 of the *Copyright Act* and *Re Royalties for Retransmission Rights of Distant Radio and Television Stations* (1990), 32 C.P.R. (3d) 97 (Copyright Board).

It must also be noted that the retransmission right contained in Section 28.01 was created only as a result of Canada's obligations under the Canada - U.S. Free Trade Agreement. Protection for copyright material contained in broadcasts originating in foreign countries has been extended on a reciprocal basis by several countries pursuant to the Rome Convention, the European Agreement on the Protection of Television Broadcasts or by mutual agreement: see, for example, the United Kingdom Copyright (Application to

a wireless signal from outside Canada is there considered to be any copyright infringement in Canada in respect of copyright works contained in that signal.[123] This could imply that that viewership of Canadian broadcasts in the United States is not an infringement of copyright in Canada. Alternatively, it could indicate that the music collective does not wish to attempt to collect royalties from transmitters outside of Canada due to administrative or other reasons. By contrast, Tariff 22 (which has not yet been approved by the Copyright Board) is specifically aimed at Internet communications and SOCAN has stated that it intends to apply Tariff 22 against both persons in Canada who send communications to recipients outside of Canada and persons outside of Canada who send communications to recipients in Canada.[124]

On balance, in view of both the wording of Section 3(1)(f) and the limited case law on this issue, the better view seems to be that a communication to the public by telecommunication takes place in Canada when such a communication is received in Canada. This means that persons who are located outside of Canada may be liable for copyright infringement in Canada if they initiate an infringing transmission which is received in Canada, but persons in Canada who communicate solely to recipients outside of Canada will not be communicating to the public by telecommunication within the meaning of the *Copyright Act*.[125]

Other Countries) Order 1993, S.I. 1993 No. 942, s. 4 and Schedule 3.

123 This is not stated explicitly in the *Copyright Act*, but must be gleaned by inference. Section 28.01 of the *Copyright Act* provides that retransmission of distant signals will not be copyright infringement if the prescribed royalties are paid, thus implying that such a retransmission would be an infringement if royalties are not paid. It must also be noted that these retransmission rights are only rights of remuneration, and not exclusive rights such as to the reproduction, performance or telecommunication rights.

124 Letter dated April 26, 1996 from SOCAN counsel to the Copyright Board. No legal rationale for this position has to date been expressed by SOCAN. Tariff 22 specifically relates to a license to communicate "in Canada".

125 This issue is discussed further below in considering who is liable for Internet copyright infringements.

4. LIABILITY FOR INTERNET COPYRIGHT INFRINGEMENT

As has been discussed above, there may be many different kinds of copyright infringement taking place on the Internet any time an unauthorized transmission of a copyright work takes place. Identifying the infringement is only the first step; perhaps more importantly, it must be determined who is liable for those infringements.

This analysis involves three stages. First, the ways in which an individual may infringe must be examined. Under Canadian law, there are two distinct types of infringement: direct infringement under Section 27(1) of any of the exclusive rights of copyright owners (which includes infringement by authorizing another person to perform an infringing act) and indirect infringement by performing one of the listed acts set out in Section 27(4). If the participation of a person in a copyright infringement does not fall within these provisions, there is no liability.[126] In addition, there may be infringements of performers' rights under Section 28.02.[127]

The second step is to analyze the roles played by the various participants in the Internet in each transmission which infringes the copyright of a work to determine which of these participants would be found to be liable for the infringement. Lastly, it must be determined if there are potential defences available in respect of Internet copyright infringements.

(a) Personal Infringement

Section 3(1) provides that direct infringement may arise either by a person doing one of the acts which fall within the exclusive right of the copyright owner (personal infringement), or by a person "authorizing" someone else to do one of those things. A fundamental difference between direct infringement (whether personal or by authorization) and indirect infringement is that Section 27(4) requires knowledge of the copyright on the part of the infringer in order for there to have been indirect infringement; there is no requirement of such knowledge for direct infringement pursuant to Section 3 and 27(1).[128]

---

126 *Apple Computer, Inc. v. Mackintosh Computers Ltd.* (1986), 28 D.L.R. (4th) 178 (F.C.T.D).

127 The definition of infringement of performers' rights under Sections 28.02(1) and 28.02(3) mirrors almost exactly the infringement definitions relating to copyright contained in Sections 27(1) and 27(4), respectively. As a result, there is no need in the analysis which follows to refer specifically to performers' rights. It must be remembered, however, that at present the exclusive rights of performers as defined in Section 14.1 are far more limited than the copyrights granted by Section 3. In particular, there is no exclusive reproduction right granted to performers.

128 *Compo Co. Ltd. v. Blue Crest Music Inc.*, [1980] 1 S.C.R. 357 at 375.

Section 27(1) describes personal infringement:

> **27. (1)** Copyright in a work shall be deemed to be infringed by any person who, without the consent of the owner of the copyright, does anything that, by this Act, only the owner of the copyright has the right to do.

Use of the word "deemed" raises a presumption of infringement when the circumstances outlined in subsection 27(1) are found to exist, subject to certain exceptions. The purpose of any "deeming" clause is to impose a meaning to cause something to be taken to be different from that which it might have been in the absence of the clause.[129] "Deemed" is an ambiguous term, and whether the presumption that is raised is conclusive or rebuttable must be determined in the context of the entire statute. In general, "where a deeming clause states the legal consequences that are to flow from described circumstances, it is *prima facie* conclusive; but where it merely states a fact that is to be presumed in described circumstances, it is *prima facie* rebuttable".[130]

Since infringement can be considered a legal consequence flowing from a given situation, the presumption is conclusive in the sense that the acts, if proven, constitute infringement.[131] As a result, so long as it is proved that a person has done any of the acts listed in Section 3(1), infringement is proven.[132]

Direct infringement may occur whether or not knowledge is present.[133] Innocent intention affords no defence, and ignorance of the existence of copyright is no excuse for infringement. "Copyright being a proprietary right, it does not avail the defendant to plead motive or intent."[134]

Many copyright infringements may be committed by individuals using physical equipment owned by others. For example, a user may upload a copy of a copyright work to a BBS. While the copy of the work is made on the server of the BBS and is retained there, it is the user which actually made the copy using the BBS's equipment. When an e-mail message containing a copy of a copyright work is sent by a user, a copy of the work will be

---

129 *R. v. Sutherland*, [1980] 2 S.C.R. 451 at p. 456.

130 Driedger, *Construction of Statutes*, (2nd ed., 1983), at p. 25.

131 Sopinka, *The Law of Evidence in Canada* (1992), ch. 4.

132 It is important to note that it is not necessary to show impairment of the copyright owner's property or even any prejudice to the owner in order to prove infringement. Even if the infringer's action were beneficial to the copyright owner, that will not absolve the infringer. There is very little room in this definition of infringement to invoke the many public policy arguments made by those advocating more freedom from liability on the Internet: see *Télé-Métropole Inc. v Michel Bishop*, [1990] 2 S.C.R. 467, at pp. 481-482.

133 See *Compo Co. v. Blue Crest Music Inc.*, [1980] 1 S.C.R. 357 at 375.

134 Fox, *The Canadian Law of Copyright and Industrial Designs*, (2nd ed., 1967), at p. 331.

made on an ISP's mail server, although it is the user which initiated the message and made the copy on the ISP's equipment.

It seems relatively clear in these circumstances that it is the user which is infringing and not the passive equipment operator such as an ISP or BBS sysop, although this issue has not been directly considered in Canadian case law. In the cases in the United States in which BBS sysops have been found liable for copyright infringement as a result of reproductions of copyright works made by users of the BBS,[135] there has been an element of cooperation or condonation by the BBS sysop which allowed the court to treat the involvement of the BBS sysop as being direct. In *Netcom*, where there was no such cooperation or condonation, liability for direct infringement was soundly rejected.[136] In order to understand the circumstances in which a person will be liable for supplying equipment which is then used to infringe, regard must be had to the Canadian law concerning "authorizing" of infringing acts.

(b) Authorizing Infringement

By virtue of Sections 3(1) and 27(1), an individual may be found guilty of direct infringement for "authorizing" the reproduction of infringing work. The copyright owner has both the sole right to do the acts enumerated in Section 3(1) and the sole right to authorize the doing of these acts by others.[137] While there is no Canadian case which deals with the issue of authorizing copyright infringement in the Internet environment, this may be the most important legal concept involved in identifying liability in Canada on the part of individual participants in the Internet environment.

The authorization right was first introduced in the United Kingdom *Copyright Act*, 1911[138] in order to diminish the effect of certain pre-1911 decisions which, based upon the language of earlier statutes which used the words "cause to", had held that a person was only liable for infringing acts committed by servants or agents. The authorization right was introduced to Canada by the enactment of Section 3(1) of the *Copyright Act, 1921*.

The phrase "to authorize" is not defined in the *Copyright Act*. English and Canadian courts have held that "to authorize" is to be understood in its ordinary sense as meaning "one who sanctions, approves, or countenances".[139] This has not posed any difficulty in the ordinary situation where the defendant is involved directly in dealing with the copyright work.

---

135 For example, see *Playboy Enterprises, Inc. v. Frena* (1993), 839 F. Supp. 4552 (U.S.D.C. Fla.) and *Sega Enterprises, Inc. v. Maphia* (1994), 857 F. Supp. 679 (U.S.D.C. Cal.). This issue is discussed in more detail below in the section on intermediary liability.

136 *Netcom*, at pp. 5-14.

137 *Compo Co. Ltd. v. Blue Crest Music Inc.*, [1980] 1 S.C.R. 357 at 376.

138 *Copyright Act*, 1911 (subsection 1(2) in fine).

139 *Underwriters' Survey Bureau Ltd. v. Massies & Renwick Ltd.*, [1938] Ex. C.R. 103 at p. 122; *Muzak Corp. v. Composers, Authors & Publishers Assn. (Canada)*, [1953] 2 S.C.R. 182 at p. 193

For example, in *Falcon v. Famous Players Film Co.*,[140] the author of a dramatic work had assigned the sole to Falcon performing right in a play entitled "Held by the Enemy" in the United Kingdom to the plaintiff. Subsequently, the author sold motion picture rights in his work throughout the world to the defendants. The defendants then produced a film based on the work in question and granted the owner of a theatre in the United Kingdom the right to exhibit the film. The Court of Appeal held that Famous Players had authorized the owner of the theatre to exhibit the film, and found them liable for the infringement of the plaintiff's performing rights.

More difficult questions are raised where the alleged infringer had supplied another person with equipment which was then employed to infringe copyright. Canadian courts have invariably held that where equipment is used by a third party to infringe copyright, the owner of the equipment does not infringe so long as the owner had no control over the manner in which the primary infringer was to use the equipment.

In *Vigneux v. Canadian Performing Right Society*,[141] the defendants had supplied a phonograph and records (an early form of jukebox) to a restaurant in return for a fixed monthly rental. The plaintiff music collective claimed that the defendants had authorized the public performance of one of their musical works which had been played on the defendant's equipment by a customer. The Privy Council held that the owners of the equipment could not be liable for authorizing the public performance of the work in question because they had no control over the use of the equipment or whether it would be made available to customers. The owner of leased equipment which is used to publicly perform a work is not authorizing the public performance.[142]

The Supreme Court of Canada reaffirmed the principles established in *Vigneux* in *Muzak Corp. v. Composers, Authors & Publishers Ass'n of Canada Ltd.*[143] Muzak was a corporation operating in the United States and had a license to make recording of certain copyright musical works. It provided recordings of some of these works to third parties in Canada. The third parties used the recordings to publicly perform the works in Canada. The plaintiff music collective, which held the Canadian performing rights to the works, claimed that, by providing the recordings to the Canadian third party, Muzak was authorizing the performance of those works in public in Canada. A majority of the Supreme Court held that a defendant must have done something more than provide the use of equipment that might possibly be used in an actual infringement of a copyright.

---

140 [1926] 2 K.B. 474 (C.A.).

141 [1945] A.C. 106 (P.C.).

142 The Privy Council made it clear that both the customer who selected the musical work to be performed and the restaurant owner who had made the equipment available to the customer were liable for copyright infringement. It is unclear from the reasons of Lord Russell whether the restaurant owner was held to be liable for having authorized the performance by the customer or as having personally infringed by the act of making the equipment available: see *Vigneux* at p. 11.

143 [1953] 2 S.C.R. 182.

> "Obviously, in one sense, Muzak authorizes Associated [the Canadian third party infringer] to make use of instruments which it owns but that use is to be in accordance with regulations dealing with it. There is not a syllable in the material to suggest that Muzak has made itself a party in interest to the performance either by warranting the right to perform without fee or by anything in the nature of a partnership or similar business relation. If by letting a device the owner is to be taken as engaging himself to its use in defiance of regulations, the very distinction between the right to make a record and the right to give a public performance by means of it which Mr. Manning made and the [*Copyright*] *Act* provides for, is wiped out. It would be as if a person who lets a gun to another is to be charged with "authorizing" hunting without a game license."[144]

Some Australian decisions adopted a different approach to the authorization issue. In *Moorhouse v. University of New South Wales*,[145] an author commenced an "test case" claiming copyright infringement against the University of New South Wales. The University had made available a photocopier for the purpose of photocopying material in the university library. A chapter of the plaintiff's book was copied using the photocopier. Although the library had taken some steps to prevent the unauthorized copying of books, there was no supervision of the use of the photocopier and the notice placed on the photocopier was less than clear and was found by the Court not to be "adequate". A majority of the High Court of Australia held that, while the University had not personally infringed the plaintiff's copyright, the University had authorized infringements of copyright because the library had extended an unlimited invitation to users to copy material in the library:

> [A] person who has under his control the means by which an infringement of copyright may be committed - such as a photocopying machine - and who makes it available to other persons knowing, or having reason to suspect, that it is likely to be used for the purpose of committing an infringement, and omitting to take reasonable steps to limit use to legitimate purposes, would authorize any infringement that resulted from its use.

---

144 *Ibid*, at p. 189; Hitchcock, "Homecopying and Authorization", 67 C.P.R. (2d) at pp. 17-49.

145 [1976] R.P.C. 151.

In another Australian case, *RCA Corp. v. John Fairfax & Sons Ltd.*[146] the court held:

> [A] person may be said to authorize another to commit an infringement if he or she has some form of control over the other at the time of infringement or, if there is no such control, if a person is responsible for placing in the hands of another materials which by their nature are almost inevitably to be used for the purpose of infringement.[147]

Such an interpretation of the "authorizing" provision of the *Copyright Act* places a positive duty on the defendant to have taken steps to prevent copyright infringement even when the defendant does not know, and may have had no contact with, the infringer. *Moorhouse* was subsequently overruled by statute in Australia.[148]

Subsequent English and Canadian case law did not follow the strict approach of the Australian courts. In *CBS Inc. v. Ames Records & Tapes Ltd.*,[149] a record shop began renting popular records to customers. It also sold blank audio tapes at a discount price. The shop was held not to be authorizing an infringing act when its customers took the records home and taped them since the shop did not sanction, approve or countenance any infringing acts by its customers. Whitford J. stated:

> Any ordinary person would, I think, assume that an authorization can only come from somebody having or purporting to have authority and that an act is not authorized by somebody who merely enables or possibly assists or even encourages another to do that act, but does not purport to have any authority which he can grant to justify the doing of the act.[150]

This distinction is important. Absent a common purpose with the personal infringer such that they are truly acting in concert, a person who takes steps to assist someone else in a copyright infringement will not be authorizing the infringement unless they purport to actually have some authority over the use of the work. As a result, if you are encouraged by a friend to make an infringing copy of a well-known work, and it is clear that the friend has no connection with the copyright owner, then the extent of the friend's urging on you to make the copy is immaterial to your friend's liability. The friend is clearly not authorizing the

---

146 [1982] R.P.C. 91 at 100.
147 *Ibid*, at 100.
148 *Copyright Act* 1968 (Cth), s. 39A, inserted by the *Copyright Amendment Act 1980*.
149 [1982] Ch. 91.
150 *Ibid*, at p. 106.

infringement since they have no ability to do so, and the *Copyright Act* does not include "incitement to infringe" the acts which are prohibited.[151]

In a series of decisions, English courts have found that the manufacturer of audio cassette decks was not liable for alleged infringements by purchasers as a result of "home taping" of pre-recorded audio cassettes. Amstrad Consumer Electronics was a manufacturer of audio recording equipment. In 1982, it introduced an audio cassette deck with twin tapes. This infuriated the U.K. music industry, which claimed (correctly) that such equipment could and would be used to make copies of copyright musical works. In 1984, Amstrad introduced a "double speed" twin deck cassette recorder, which allowed copying to be done faster than the speed of playing the tape. The British Phonographic Industry Limited (BPI), a record industry lobby group, and others complained to Amstrad that, by advertising and selling the twin deck cassette recorders, Amstrad was authorizing copyright infringement by purchasers of the equipment who used it to do home taping. After inconclusive negotiations, Amstrad brought an action seeking a declaration that it was not authorizing copyright infringement by selling the twin deck cassette recorders.

It was not contested that Amstrad knew that the majority of the purchasers of their machines would use them to unlawfully copy pre-recorded cassettes, and in fact Amstrad's advertising of the tape deck had emphasized this feature. The trial judge (who was also the trial judge in the *C.B.S v. Ames* case) was critical of Amstrad and refused to declare that Amstrad was not authorizing infringement.[152] The Court of Appeal[153] disagreed. It held that the Australian High Court in *Moorhouse* had inappropriately chosen synonyms for the word "authorize" which expanded the meaning of the statutory provision. The Court applied the rule in *Vigneux* and held that Amstrad had no responsibility for the use of the cassette decks once they had been sold.

> "None of the authorities which have been cited to us have persuaded me that the word bears any other meaning in section 1 of the Copyright Act 1956. The very essence of a grant or purported grant of this

---

151 *Ibid*, at p. 118. It is interesting to note that Whitford, J. did not disapprove of the decision of the High Court of Australia in *Moorhouse*, but merely distinguished it on the basis that the record shop was not lending out the equipment for home taping at the same time as lending the records. Because *Vigneux* was a Privy Council case and not binding on Whitford, J., he expressed some doubt that the defendant in that case should have escaped liability since it did provide the record player as well as the records. *Vigneux* is binding on Canadian courts, and it is difficult to conclude that supplying both the equipment which is employed to infringe and a legal copy of the work to be infringed could be found to be "authorizing" the infringement in the normal course.

Exclusive rental rights have been granted to computer program copyright owners by Section 3(1)(h) of the *Copyright Act*.

152 *Amstrad Consumer Electronics PLC v. The British Phonographic Industry Limited*, [1986] F.S.R. 159.

153 *Amstrad Consumer Electronics PLC v. The British Phonographic Industry Limited*, [1986] F.S.R. 201.

> nature is that the grantor has some degree of actual or apparent right to control the relevant actions of the grantee. In the present case it has not been alleged, and could not be alleged, that Amstrad has any actual or apparent right to control the relevant actions of members of the public who, having purchased its machines, subsequently use them in such manner as to infringe the copyright of B.P.I.'s members. This renders the present case a quite different one from the Australian case of *Moorhouse v. University of New South Wales* [1976] R.P.C. 15 on which Mr. Kentridge relied as his strongest authority. In that case, unlike the present, as Lawton L.J. has pointed out, the University were at all material times in a position to control the use of the photocopying machine which had been used to infringe copyright, so that the evidence may well have warranted a finding of implicit authorization.
>
> The highest that the present case can be put on the facts is that, as the learned judge found (at page 59G of his judgment) Amstrad "in selling these units are intentionally placing in the hands of purchasers a facility which they must know is inevitably going to be used for the purposes of infringement." Even accepting this strong finding of fact, it would not, in my judgment, justify a finding of "authorization" in the relevant sense as a matter of law."[154]

In subsequent proceedings, the Court of Appeal struck out BPI's statement of claim.[155] The House of Lords[156] agreed. In doing so it distinguished *Moorhouse* and rejected the portion of the *RCA Corp.* case cited above as having been "stated much too widely".[157] Although the sale of the tape decks placed in the hands of the public "materials which by their nature are almost inevitably to be used for the purpose of an infringement" by copying pre-recorded material, Amstrad only was facilitating infringement, but did not authorize it.

> "... There is nothing express or implied in the Act which inhibits the invention, manufacture, sale or advertisement of electronic equipment capable of

---

154 *Amstrad, supra*, at pp. 211-212.

155 [1986] F.S.R. 201.

156 *CBS Songs Ltd. v. Amstrad Consumer Electronics Plc*., [1988] 2 All E.R. 484 (H.L.).

157 *CBS Songs*, at p. 494.

> lawful or unlawful reproduction.
>
> ... BPI submit that by selling a model which incoporates a double-speed twin-tape record Amstrad "authorise" the purchaser of the model to copy a record in which copyright subsists and therefore Amstrad does not infringe the exclusive right of the copyright owner. My Lords, twin-tape recorders, fast or slow, and single-tape records, in addition to their recording and playing functions, are capable of copying on to blank tape, directly or indirectly, records which are broadcast, records on discs and records on tape. Blank tapes are capable of being employed for recording or copying. Copying may be lawful or unlawful. Every tape recorder confers on the operator who acquires a blank tape the facility of copying; the double-speed twin-tape recorder provides a modern and efficient facility for continuous playing and continuous recording and for copying. No manufacturer and no machine confers on the purchaser authority to copy unlawfully. The purchaser or other operator of the recorder determines whether he shall copy and what he shall copy. By selling the recorder Amstrad may facilitate copying in breach of copyright but do not authorize it."[158]

As a result, even where the defendant knows that its equipment is going to be employed for infringing purposes, it will not be liable if it has no control over the use being made of the equipment, and it does not purport to give the personal infringer a license or permission to infringe.[159]

---

158 *Ibid*, at p. 492.

159 Although it is dangerous to give much weight to decisions from the United States because their copyright statute is quite different from Canada's, it must be noted that a similar principle was enunciated in *Sony Corporation v. Universal City Studios*, 464 U.S. 417 (1984), in which the Supreme Court held that manufacturers of video cassette recorders were not liable for contributory copyright infringement by home tapers of pre-recorded video cassettes or television broadcasts. The Court relied heavily on the fact that the recorders could be employed for significant non-infringing uses such as "time shifting" of television programs. The U.S. concept of "contributory infringement" is taken from tort principles which have not been applied in Canadian copyright law; for a possibly contrary view, see Elrifi, "What's DAT - Armstrad Revisited: Canadian Copyright Law and Digital Audio Tape Players", 14 Can. Bus. L.J. 405 (1988), at pp. 416-418.

In *Sega Enterprises v. Maphia* (1994), 857 F. Supp. 679 (U.S.D.C. Cal.), at paras. 35-38, it was held that the sale of video game copiers which could not be used for any lawful purpose would be contributory infringement. See also *Atari, Inc. v. JS & A Group, Inc.* (1983), 597 F. Supp. 5 (N.D. Ill.).

In the *CCTA* case,[160] the Federal Court of Appeal held, in an *obiter* passage, that, by sending television signals containing copyright music, cable operators were authorizing infringing public performances by customers.[161] This decision is not inconsistent with the case law cited above, since it was clear that the cable operators were aware that the signals they were sending to their customers contained copyright works. In addition, the cable operators were doing more that merely providing equipment for the use of customers; they were assembling a collection of stations and signals and marketing them to customers on a "one-to-many" basis.

In *de Tervagne v. Beloeil (Ville de)*,[162] the Federal Court dealt with a claim against several individuals and organizations who were involved in the unauthorized presentation of a play, the performing rights to which were owned by the plaintiffs. After reviewing the relevant cases, Joyal, J. concluded that, in view of the decision in *Vigneux*, the Australian decisions in *Moorhouse* and *RCA Corp.* must be rejected in Canada. In order to "authorize", a person must sanction, approve or countenance something more than the mere use of equipment that might possibly be used to infringe a copyright. Otherwise, it will be presumed that the person authorized the activity only so far as the activity is in accordance with law.[163]

The "something more than mere use" that must be sanctioned, approved or countenanced does not need to go so far as to grant, or purport to grant, a right. It is possible to establish that a person has sanctioned, approved, or countenanced an infringing activity if it is shown that certain relationships existed between the alleged authorizer and the actual infringer, or that the alleged authorizer conducted himself in a certain manner. The most obvious such situation will be in the employment context. This is a matter of fact that depends on the circumstances of each case.[164] In analyzing the facts of the *de Tervagne* case, Joyal, J. stated:

> "... The question of authorization is a question of fact in each case. In this case, the producer of the play, Mr. Bossac, alone had control over the play. The other defendants were not in such a position as would have enabled them to authorize the infringement. The mere fact that the Town of Beloeil and Les Productions de la Coulisee rented the hall to Mr. Bossac, even though this in a way made possible or facilitated the infringement, does not support a finding that they authorized the performance of a play which

---

160 *CCTA v. Copyright Board* (1993), 46 C.P.R. (3d) 359 (F.C.A.).

161 *CCTA*, at pp. 371-372. This decision pre-dated the amendments to the *Copyright Act* which made cable television programming a communication by telecommunication.

162 (1993), 50 C.P.R. (3d) 419 (F.C.T.D.).

163 *de Tervagne, supra*, at p. 433.

164 *de Tervagne, supra*, at p. 436.

> infringed copyright. The defendants could reasonably have assumed that the purpose of renting the hall was to present a play in a lawful manner. Much more would be needed, according to the reasoning set out in *Vigneux* or in *Muzak*, for us to find the defendants liable. The participation of the defendants Ilial and Neveu was strictly in their relationship as employees of Mr. Bossac. They were at all times subject to his authority."[165]

Lastly, it is unclear whether an act of authorization which takes place outside of Canada can be the basis of a claim of infringement in Canada, even if the primary act which is authorized is done in Canada.[166]

The rationale of the case law relating to "authorizing" infringement can be summarized as follows:

a) the owner of equipment which is used to infringe does not authorize the infringement by supplying the equipment. Even if the owner knows that the equipment will be used to infringe, the owner will not be authorizing infringement so long as the owner does not have control over the infringer's use of the equipment;[167]

b) in order to create liability on the part of a defendant, any authorization by the defendant must be of the infringing activity itself, not of activity which could be either infringing or non-infringing. The court will not presume that the defendant intended to authorize infringing activity if the scope of the activities authorized included non-infringing activities;[168]

c) the analysis of the facts in each case will be determinative. If the defendant took active steps to

---

165 *de Tervagne, supra*, at p. 437.

166 Skone James, *Copinger and Skone James on Copyright*, (13th ed. 1991), at ¤8.142

167 While the American copyright law concept of contributory infringement is not identical to the Canadian concept of "authorization", there are some similarities. In *Netcom*, the court decided that there was a triable issue concerning whether Netcom permitted its facilities to continue to be used to disseminate the infringing material after receiving notice of the infringement: *Netcom* at pp. 16-18.

168 See the discussion in Elrifi, "What's DAT - Armstrad Revisited: Canadian Copyright Law and Digital Audio Tape Players", 14 Can. Bus. L.J. 405 (1988), at pp. 415-416.

> prevent an infringement, or had no knowledge of the possibility of an infringement, it is much less likely that the defendant could be found to have authorized the infringement.[169]

The relative narrowness of the concept of "authorization" in Canadian law is of great importance in the Internet environment. Much of the infringement which takes place on the Internet will be done as a result of users giving commands which result in reproductions or communications of copyright works through the use of equipment which is provided by ISPs and other intermediaries. It is clear that such equipment can be used, and is in fact used, for non-infringing purposes. Therefore, absent a common purpose with the users, ISPs, as the suppliers of such equipment, should not be liable for infringement caused by its users any more than the seller of cassette recorders.[170]

(c) Indirect Infringement

Section 27(4) of the *Copyright Act* describes indirect infringement as follows:

> 27.(4) Copyright in a work shall be deemed to be infringed by any person who
>
> (a) sells or lets for hire, or by way of trade exposes or offers for sale or hire,
>
> (b) distributes either for the purposes of trade or to such an extent as to affect prejudicially the owner of the copyright,
>
> (c) by way of trade exhibits in public, or
>
> (d) imports for sale or hire into Canada,
>
> any work that to the knowledge of that person infringes copyright or would infringe copyright if it

---

169 It must be noted that the law in this area is still developing, and predicting the outcome of Internet cases is fraught with uncertainty. The recent action by several of Canada's cable channels against suppliers of "gray market" direct-to-home satellite dishes appears to challenge the rule that the supply of equipment only cannot be "authorizing" copyright infringement. It is possible, however, that the dishes being sold cannot be used for a non-infringing use because there is no transmitter to the dish which has a Canadian license to transmit the works.

170 This issue is discussed in more detail below in the section on intermediary liability.

had been made within Canada.[171]

Indirect infringement under Section 27(4) cannot be authorized by a third party since the acts which constitute indirect infringement are not within the acts enumerated in Section 3(1) of the *Copyright Act* to which the copyright owner has an exclusive right.[172]

A distinguishing feature of indirect infringement is that knowledge on the part of the infringer that copyright is being infringed is required. An alleged indirect infringer must have knowledge that the work dealt with infringes copyright. The burden of proving the knowledge of the defendant rests upon the plaintiff, and that burden has been described as a heavy one.[173] However, Section 27(4) must be read in conjunction with Section 39, which states that, if at the date of the infringement the copyright in the work was duly registered pursuant to the *Copyright Act*, a defendant will be deemed to have had reasonable grounds for suspecting that copyright subsisted in the work.[174] Where knowledge is an essential element of infringement, ignorance may constitute a valid defence.[175]

In *Clarke, Irwin & Co. v. C Cole & Co. Ltd.*[176] and *Simon & Schuster Inc. v. Coles Book Stores Ltd.*,[177] the term "knowledge" in Section 27(4) was held to mean that which would suggest to a reasonable man that a breach of copyright was being committed.[178] These cases conclude that "knowledge" in comparable contexts means notice of facts such as would put a reasonable person on enquiry.[179]

Once an individual has either actual or imputed knowledge that the work dealt with may be infringing copyright, the individual has an obligation to make enquiries to ensure that the work does not infringe copyright. In *Simon & Schuster*, the court held that an importer of a book had knowingly infringed copyright. The court determined that the printed notice in the book was sufficient to put a prudent dealer on inquiry as to whether the parties were entitled to copyright protection and right of resale, and therefore the defendant should have taken steps to ensure that he was not dealing with an infringing work. The defendant's attempt to evade liability by "closing his eyes" as to the rights of the parties was unsuccessful.

---

171 These dealings may also constitute criminal offences, as provided for in section 42(1) of the *Copyright Act*.

172 Skone James, *Copinger and Skone James on Copyright*, (13th ed. 1991), at ¤8.134; *91439 Canada Ltee. v. Editions JCL Inc.* (1992), 41 C.P.R. (3d) 245 (F.C.T.D.).

173 *Infabrics Ltd. v. Jaytex Shirt Co. Ltd.*, [1978] F.S.R. 451; *Sillitoe v. McGraw-Hill Book Co.*, [1983] F.S.R. 545.

174 Richard, "Concept of Infringement in the *Copyright Act*", in Henderson, *Copyright Law of Canada* (1994), at p. 211.

175 Skone James, *Copinger and Skone James on Copyright*, (13th ed., 1991), at pp. 240-242.

176、 (1959), 33 C.P.R. 173 (Ont. H.C.J.).

177 (1975), 9 O.R. (2d) 718.

178 *Clarke, Irwin, supra*, at p. 181.

179 *Apple Computer, Inc. v. Mackintosh Computers Ltd.* (1986), 28 D.L.R. (4th) 178 (F.C.T.D.), at p. 225.

A defendant is not entitled to overlook obvious indications of copyright infringement.[180]

But, conversely, knowledge is not sufficient to show indirect infringement where none of the enumerated acts have been committed. Where an individual financed an operation which he knew was infringing copyright, but had not done any of the acts listed in Section 27(4) and could not have been seen to have been authorizing the infringement, he was found not to be liable for infringement.[181]

The concept of indirect infringement can be important in dealing with BBS sysops and other Internet intermediaries which permit their equipment and systems to be used specifically for infringements which fall within Section 27(4).[182] If the intermediary is put on notice of an infringement and takes no reasonable steps to prevent its continuation, the intermediary may be liable for indirect infringement.

(d) Who Infringes on the Internet?

The application of all of the law discussed above to individual Internet participants is difficult because there are large variations in the roles taken by various participants at different times in respect of different transactions. Each case will turn to some extent on its own facts. A useful categorization can be made, however, between three groups: posters, recipients and intermediaries.

A poster places copyright content on the Internet in such a way that it can be accessed by others. This may involve sending an e-mail message, posting a message to a newsgroup, uploading a work to a BBS's server, including a work in a Web page, or placing a copy of a work in a library area of an on-line service.

A recipient is anyone who receives a work. A work need not be viewed or heard to be received, since a copy of a work can be downloaded to storage by a recipient computer but never accessed for viewing by its owner or operator.

Intermediaries consist of a wide range of individuals and organizations with one common function: they provide the link between posters and recipients. Intermediaries can be telecommunications carriers, BBS sysops, ISPs, on-line services and various other technical providers. Intermediaries are the owners and operators of the equipment and systems which posters and recipients employ to communicate with each other.

These characterizations are by no means exclusive or watertight. Most Internet participants would at one time or another have been both posters and recipients. Many

---

180 *Simon & Shuster, supra*, at p. 720.

181 *Apple Computer, supra*, at pp. 226-227.

182 See the discussion relating to intermediary liability below.

intermediaries from time to time perform roles as posters or recipients. This should not confuse the issue. Each infringing Internet transmission must be examined individually to determine what role is played by each participant. It does not matter, for example, whether an ISP is a poster in respect of non-infringing Internet communications if its role in the infringing Internet communication being examined is that solely of an intermediary.[183]

(i) Liability of Posters

The easiest analysis involves persons who post unauthorized copies of a copyright work in Canada to BBSs, newsgroups or Web sites located in Canada, or e-mail such copies to recipients located in Canada. In the process of posting or e-mailing such copies, there must have been an infringing reproduction of the work in violation of Section 3(1)(a). Because the poster is the person causing the copies to be made, albeit perhaps by employing equipment belonging to others, he or she is clearly guilty of infringement of the reproduction right.[184]

The situation is less clear if the computer on which the poster places the unauthorized copy is located outside of Canada. Because the copying does not take place until the infringing copy is reproduced or fixed, it would appear that there is no infringement of the reproduction right in Canada.[185]

---

183 It is easy to drift from an analysis of each individual communication to an analysis of the overall role generally played by an Internet participant. The IHAC Copyright SubCommittee stated that "electronic bulletin board operators are liable for copyright infringement since they are not common carriers" (IHAC Copyright Report, p. 16). It is possible that the IHAC Copyright SubCommittee was meaning to refer to Section 3(1.3) of the *Copyright Act* and its exception to infringement by communication to the public by telecommunication, but that provision does not refer to "common carriers": see the IHAC Report at page 120.
There appear to be several additional layers of analysis of this issue:
(a) what rights is it alleged are being infringed by the BBS sysop?
(b) what actions is the BBS sysop performing which could lead to liability for the infringement of such rights?
(c) what is a "common carrier" and what effect, if any, does that status have on liability for copyright infringement?
(d) can the BBS sysop rely on the exemption in Section 3(1.3) of the *Copyright Act*?
"While a service provider could, for instance, put up its own World Wide Web pages, the effect of doing so should be kept distinct from the provider's conduit services": Loundy, "Revising the Copyright Law for Electronic Publishing", 14 J. of Comp. & Info. Law 1 (1995), at p. 41.
These issues are discussed further below under the heading "Liability of Intermediaries".

184 Earlier in 1996, a company in Dallas began to offer "music on demand" over the Internet under the name AudioNet. The Recording Industry Association of America (RIAA) demanded that the AudioNet service be discontinued until its operators obtained licenses to perform the recordings. AudioNet's position that it was acting as a radio service (and had paid royalties to ASCAP an BMI on this basis) would offer no defence under Canadian law since a reproduction license would still be required from the copyright owner of the musical works (the composer) and the recordings of the performances of those works (the record company). See "RIAA Addresses C'Right Allegations", *Billboard*, March 16, 1996, p. 5.

185 In most cases, the poster will have infringed the reproduction right prior to posting the copy over the Internet (such as by scanning a photographic work or by saving an infringing copy on the poster's own computer) and will still be subject to an action for infringement by the copyright owner. Because this study is limited to

It must next be considered whether a poster communicating a copyright work to a location outside of Canada has infringed the right to communicate to the public by telecommunication within the meaning of Section 3(1)(f). As noted above, the *Copyright Act* does not indicate where a communication to the public by telecommunication takes place in an international transmission on the Internet. The better view seems to be that a communication to the public by telecommunication takes place in Canada when such a communication is received in Canada. As a result, a poster in Canada sending a message solely to an e-mail address or addresses outside of Canada would not be communicating a work to the public by telecommunication in Canada, even though the message originated in Canada.

The next issue is whether posters who are located outside of Canada can be liable for copyright infringement in Canada if they initiate an infringing transmission which is received, or is capable of being received, in Canada.[186] When a poster located outside Canada sends an e-mail to a sufficient number of Canadian addresses,[187] it would appear clear that this is a communication to the public by telecommunication in Canada. There is both the actual communication to the public in Canada and the intention to communicate to the public in Canada.

Where a poster outside of Canada posts a message on a newsgroup or places it on a BBS or Web site, where it is generally available to recipients in Canada, that would also appear to be a communication to the public by telecommunication in Canada since it can be received by someone in Canada even though the server on which the copy of the work is made may be located outside of Canada.[188] It is unclear whether it is necessary that the foreign poster had any intention that the transmission reach a recipient in Canada.[189]

In addition, in most cases either posting a copy of a unauthorized work to a

---

liability arising from Internet use, this potential liability is not analyzed any further.

186 Of course, just because there may be liability in Canada does not mean that there will be any meaningful recourse against the foreign infringer since they may simply stay out of the jurisdiction of Canadian courts.

187 Note that the poster may not know the message is going to a Canadian recipient if a remailer is being used.

188 Since any Web or Usenet site can be accessed by users in Canada, it would appear that any posting is a communication to the public in Canada. There might be exceptions if a BBS could not be accessed by anyone outside of a specific area code or other geographic area, but such restrictions are rare.

A recent decision in the United States appears to have taken a similar approach. In *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.* (S.D.N.Y. No. 79), Cv. 3525, June 19, 1996), it was held that an Italian Web site violated an earlier injunction prohibiting the use of "PLAYMEN" on a magazine "published, distributed or sold in the United States". See Loundy, "E-Law: Reach Out and Sue Someone", 1-7 *Cyberspace Lawyer*, October 1996, page 19. This area is still unclear under U.S. law. "The jurisdiction of U.S. courts does not extend to sysops who operate in other countries.": Meyer, "National and International Copyright Liability for Electronic System Operators", available at http://law.indiana.edu/glsj/vol2/no2/meyer.html.

189 See the discussion above of the *International Good Music* case.

newsgroup or placing it on a BBS or Web site may constitute indirect infringement under Section 27(4) if the requisite element of knowledge is present. Such a posting could be seen to be a distribution of the work "to such an extent as to affect prejudicially the owner of the copyright", or could be a public exhibition if it is "by way of trade".

The result of this analysis is that Canadian copyright law would seem to be able to cast a wide net to find liability on the part of posters, even those located outside of Canada.[190] The difficulty facing copyright owners has been that Internet posters of unauthorized copyright materials are often impossible to locate and infringement actions against such individuals are usually not cost-effective.[191] As a result, copyright owners have tended to look elsewhere in the Internet transmission chain to attempt to obtain compensation for infringing activities.

(ii) Liability of Recipients

The *Copyright Act* focuses, quite correctly, on actions taken by the disseminators of unauthorized copyright works, and it is the person who supplies the unauthorized copies to others that is the main target of most restrictions.[192] It is difficult to see how a member of the public who is a recipient of a communication to the public by

---

190 It should be noted that this is not an extraterritorial application of Canadian law, since what is being targeting is communications to the public in Canada. It may come as a surprise to a person in Vietnam who has posted an infringing copy of a work to a local-interest newsgroup on the Internet that they have thereby infringed that copyright in Canada. The fact is that an Internet posting may be a copyright infringement in many countries simultaneously. As noted above, this analysis does not take into account the issue of which law should be applied in determining whether the posting was in fact an infringement. Some authors have argued that courts should apply the law of the country in which the posting occurs. This raises the possibility that infringers would simply seek out the "least protective country" and communicate to the entire world from such a "pirate haven": see Geller, "Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Network World", 20 Columbia-VLA Journal of Law & The Arts 571 (1996), at p. 572.

191 "Often, those who are most responsible for the piracy are ingenious in their ability to hide their illegal activities from the authorities. Individuals who engage in direct file transfer from one computer to another are often impossible to detect. This is one of the reasons that bulletin board operators are a preferred target in infringement actions.": Axe, "Computer Bulletin Boards and Software Piracy: Are System Operators to Blame for Copyright Infringement by their Users?", *1996-97 Entertainment, Publishing and the Arts Handbook* 141 at p. 156.

192 Thus, for example, there is no infringement of copyright by the purchaser or possessor of infringing copies of a work. What is prohibited is reproducing a copyright work (Section 3(1)) and selling, hiring or offering to sell or hire an infringing work (Section 27(4)), all of which are done by the supplier of unauthorized copies. The only possible exception is the summary conviction offence in Section 42(2)(a) for possession of a "plate for the purpose of making infringing copies". It is unclear from the definition of "plate" in Section 2 whether computer storage devices could be seen to be a "plate". Bill C-32 proposes to amend the definition of "plate" to include "any matrix or other appliance used or intended to be used for making or reproducing sound recordings, performer's performances or communication signals", which would appear to be an extension of the current offence and could include the possession of a computer hard drive onto which infringing copies of such works have been downloaded.

telecommunication can be said to have infringed on the copyright of the owner of the work pursuant to Section 3(1)(f). The communication of the infringing copy is made "to the public", not "by the public", which implies that the person performing the infringing act is the poster, not the recipient.

As a result, any liability on the part of an Internet recipient of an unauthorized copy of a copyright work must arise from either the acts surrounding the reception of the work (such as the reproduction of the work by the recipient in order to view it) or from the relationship between the poster and the recipient. If there is some pre-existing relationship between the poster of an unauthorized work and the recipient such that the recipient was being sent the work as part of a scheme to distribute or reproduce copies of the work, then it is possible that the recipient could be seen to be in a joint venture with the poster such that the recipient is also communicating the work to the public by telecommunication. For example, an organized group of individuals which exchanges unlicensed copies of computer software or photographs could be seen to be in a joint venture with the other members of the group. In addition, it is likely that all members of such a group would be guilty of indirect infringement pursuant to Section 27(4).[193]

In addition, the recipient could take steps to further disseminate the work to the public (such as by placing the unauthorized copy on a large screen to be viewed by a large group), and this could constitute a separate public performance of the work.

As has been discussed earlier, it likely is not possible for a person to receive an unauthorized copy of an copyright work over the Internet without reproducing the work in violation of Section 3(1)(a). If the work is viewed or, in the case of a computer program, loaded into memory, a copy is made, however fleetingly, in the RAM of the recipient's computer.[194] In order for there to be infringement, it is not necessary that the recipient have any knowledge or warning that what is being accessed is infringing copyright.[195]

(iii) Liability of Intermediaries

It is the potential liability of intermediaries on the Internet which has caused the greatest debate, both in assessing the nature and scope of the liability and in the potential problems caused by such liability. Because of the difficulty in locating and stopping individual posters and recipients from continuing infringing activities, copyright owners have in some cases turned to the intermediaries which provide the connection between posters and

---

193 As discussed below, this could also be the basis for the liability of a BBS sysop or on-line service which was involved in such exchanges.

194 See discussion at footnote 76.

195 While there would seem to be little chance that an innocent private recipient of unauthorized copyright material could actually be sued by the copyright owner, it does seem to be counter-productive to have the law apply in such a way that every Internet user is potentially a copyright infringer.

recipients.[196] The question is whether such intermediaries are themselves infringing copyright and, if so, in what circumstances.

At first glance, it would appear that the simplest analysis relates to true "carriers" of Internet transmissions which pass along electronic messages without copying or altering those messages. Such carriers would include the telephone companies and other entities along whose systems Internet transmissions flow. Many commentators assume that such carriers have no liability for the content of the electronic information which they carry along their systems, but do not analyze critically why this is so.[197]

"Common Carriers"

While commonly referred to in Canada, the concept of a "common carrier" exemption from liability is an unfortunate and inaccurate importation of certain United States legal doctrines which have never been recognized in Canada. There is no general "common carrier" rule in Canadian law which would provide protection to either telecommunications carriers or ISPs from liability for copyright infringement which occurs as a result of their Internet activities. While, as discussed below, the exception contained in Section 3(1.3) of the *Copyright Act* may limit the liability of ISPs somewhat, ISPs will continue to be liable if they infringe the reproduction right. Since there is such a wide misconception about the role and liability of common carriers in Canadian law, some further analysis is required.

Even the law in the United States, which appears to recognize a general limitation on intermediary liability in some situations and has a somewhat wider copyright "common carrier" defence than is provided by Section 3(1.3) of the *Copyright Act*, likely does not now exempt all ISP activity from liability for Internet copyright infringement.[198]

The United States "common carrier doctrine" is often confused with the common law restriction on intermediary liability. The common carrier doctrine in the United States has developed from the law relating to persons providing a public good, such as an inn keeper or a ferry operator.[199] In certain circumstances where a person is "holding out" (a voluntary undertaking to provide a service for hire to the public) and was exercising monopoly power, that person could be required to provide service to all comers on a non-

---

196 "It may be difficult, or impossible, to determine who is responsible for on-line infringement of copyrighted works. The direct infringers are often home users, and they may be impossible to find. Internet communication is largely anonymous. The on-line services may be much easier to find, but they may not be legally responsible for the actions of their customers. Thus, the true challenge to the copyright owner may not be determining which rights have been infringed, but rather determining the proper defendant."
Segal, "Dissemination of Digitized Music on the Internet: A Challenge to the Copyright Act", 12 Santa Clara Comp. & High Tech. L.J. 97 (1995), at p. 124.

197 See the IHAC Copyright Report, p. 16 and the IHAC Report, p. 120.

198 Perritt, "Law and the Information Superhighway" (1996), at pp. 164-166; 178-179.

199 Perritt, *supra*, at p. 45.

discriminatory basis.[200] Not only did "common carrier" status not provide a blanket exemption from liability while carrying passengers or cargo, in some circumstances a common carrier was held to a "heightened standard of care" in assessing its tort liability.[201] Much of the relevance of the common carrier status in the United States has been eliminated over the past century by regulation of major monopoly services in the transportation industry.[202]

What is commonly known as the "common carrier doctrine" in referring to liability issues is in fact an application of fault-based tort concepts to entities such as telegraph and telephone companies which also have been historically known as "common carriers".[203] In certain fault-based torts, such as defamation, courts in the United States have held that a conduit or intermediary which lacks control over, and does not vouch for, the content of its transmissions may be exempted from liability because the conduit is not at fault.

> "The difficulty and inconvenience of requiring the operators to analyze either the message or the senders from either a factual or legal standpoint is manifest. The indispensability of the telegraph, on the other hand, is as unchallenged as the realization that speed is the essence of its worth. Telegraph companies operated under statutes subjecting them to penalties and fines for discrimination and negligent transmission. The pressure and responsibility thrust upon the companies by these statutes are unbearable unless the companies can comply without subjecting themselves to a libel action."[204]

Part of the rationale for this rule arises from the fact that many such conduits are in fact common carriers and therefore required to accept all traffic brought to them without discrimination. Later cases have made the same point in respect of telephone companies.[205]

---

200 A similar doctrine was applied in Canada in respect of common carriers of goods, but not passengers: see *Direct Transport Ltd. v. Detroit Windsor Ferry Co. Ltd.*, [1936] O.R. 86, aff'd. [1936] 4 D.L.R. 807 (Ont. C.A.) and *Kent v. Petrine*Ê(1914), 6 W.W.R. 1111 (B.C.)

201 *Alpha Zeta Chapter of Phi Cappa Alpha v. Sullivan*, 740 S.W. 2d 127 (Ark. 1987); *Summers v. Montgomery Elevator Co.*, 757 P. 2d 1255 (Kan. 1988); Perritt, *supra* at p. 47.

202 Ultimately, telegraph companies were found not be common carriers by the United States Supreme Court: *Primrose v. Western Union Telegraph Co*., 14 Sup. Ct. Rptr. 1098 (1984).

203 Perritt, *supra*, at pp. 164-166. See also *Netcom* at p. 8, where Netcom's claim that it was entitled to immunity as a common carrier was rejected.

204 Martin, "Telegraphs and Telephones", 2 Wash. & Lee L. Rev. 141 at 147 (1940); *O'Brien v. Western Union Telegraph Co.*, 113 F. 2d 539.

205 *Anderson v. New York Telephone Co.*, 320 N.E. 2d 647 (N.Y.C.A. 1974); Note, "Must the Telephone Company Censor to Avoid Liability for Libel?", 38 Alb. L. Rev. 316 (1974).

The same rule does not apply to copyright infringement in the United States, however, because it is not based in tort and is not primarily fault-based.[206] Instead, Section 111 (a)(3) of the *United States Copyright Code* provides that a "secondary transmission"[207] which contains a performance or display of a copyright work is not an infringement if

> "the secondary transmission is made by any carrier who has no direct or indirect control over the content or selection of the primary transmission or over the particular recipients of the secondary transmission, and whose activities with respect to the secondary transmission consists solely of providing wires, cables, or other communications channels for the use of others."

This exemption has been held not to be applicable to an ISP.[208] If an ISP or on-line service is active in monitoring or controlling the content of the secondary transmissions on its services, then it is unlikely to be able to say that its activities in respect of the transmissions "consists solely of providing wires, cables or other communications channels". It is also unclear whether the services provided by an ISP or on-line service to facilitate the transmission of messages to and from its subscribers would fall within the definition of "communications channels".

Section 111(c)(3) of the *United States Copyright Code* appears to be specific to individual transmissions. The extent of an ISP's activities must be examined in relation to each individual transmission which includes an unauthorized copyright work. Even if an ISP provides other services to its subscribers in respect of other transmissions (such as preventing the delivery of such other transmissions as a result of copyright, defamation or obscenity concerns), the ISP has still done nothing in respect of those transactions which it permits to pass through except "provide communications channels" for those transmissions. Like Section 3(1.3) of the *Copyright Act*, Section 111(c)(3) of the *United States Copyright Code* only deems the performance or display of the work not to be an infringement. There is no exemption in respect of any reproduction of a copyright work.

Canadian law has never adopted the "common carrier" exemption which the United States law applies to fault-based torts.[209] In an early case, the Supreme Court of

---

206 Perritt, *supra*, at pp. 165-166.

207 The term "secondary transmission" is defined in Section 111(f) of the U.S. *Copyright Code* in such a way that it appears to be intended to refer to television broadcasting, but it is unclear whether the provision will be interpreted so narrowly.

208 *Netcom*, at p. 8.

209 See Ryan, "Canadian Telecommunications Law and Regulation" (1993) at p. 4-6:

> "While the term "telecommunications common carrier" has now achieved currency in Canada, there is no jurisprudence to support

Canada affirmed a trial judgment against a telegraph company which it transmitted a libelous message which had subsequently been published in a newspaper.[210] Ritchie, C.J. stated (at pp. 258-259):

> "... To say that the transmission of such news by telegraph companies over telegraphic lines is not a legitimate branch of their business, and a large source of revenue is to ignore what is presented before our eyes every day, when we take up a morning or evening paper. To say that we can suppose that all such news is transmitted by such company gratuitously for the pleasure of operating, or for any love the company bear either the publishers who print or the public who read newspapers, or from any philanthropic desire to spread intelligence, and to say that they can transmit, nor correct statements, but whatever so called news or rumours they may collect, or what may be collected for them by others of a sensational character, without regard to its truth or falsity or libelous character, and so derive a large revenue and not be responsible to those who may be injured, or possibly ruined by such participation in the publication of gross libels, and which libels would not and could not be published but through their instrumentality, would be simply to stultify ourselves. Can it be possible that the character and business of innocent persons can be destroyed because the libelers, with a view to gain and the extension of their business, choose to transmit over their lines statements and rumours unfounded in fact in relation to the private character or business standing of individuals with whom they have no connection, and with whose character or business they have no right to meddle, and when no duty, legal, moral or social is cast upon them to promulgate the statements or rumours, and the aggrieved parties shall have no remedy against them? The law has not, and I am full well assured never will, sanction such an idea. ...

> the notion that there has been any change in the common law liability of these carriers, and it would be unwarranted to read into the provisions of the statutes that have employed the term any legislative intention to alter the rules governing liability."

210 *Dominion Telegraph Company v. Silver* (1882), 10 S.C.R. 136.

> To exempt telegraph companies from liability as now claimed would be to clothe them with an irresponsible power for the perpetration of injustice and wrong wholly opposed to every principle of law or right."

The *Dominion Telegraph* case has not been revisited by the Supreme Court of Canada.

It is unclear whether modern telecommunications carriers would be dealt with in the same way as telegraph services. The argument is made that telephone carriers, for instance, do not "transmit" messages in the way that telegraph operators did; rather, it is the customer who "transmits" the message through the telephone company's equipment.[211]

The liability of telecommunications carriers in Canada has been dealt with in a limited way by statute and regulation. Section 16.2 of the Terms of Service[212] provides as follows:

> "The [carrier] is not liable for:
>
> (a) any act or omission of a telecommunications carrier whose facilities are used in establishing connections to points which [the carrier] does not directly serve;
>
> (b) defamation or copyright infringement arising from material transmitted or received over the carrier's facilities;
>
> (c) copyright or trademark infringement, passing off or acts of unfair competition arising from directory advertisements furnished by a customer or a customer's directory listing, provided such advertisements or the information contained in such listings were received in good faith in the ordinary course of business."

Thus, regulated Canadian telecommunications carriers have been exempt from liability for copyright infringement while providing telecommunication services.[213]

---

211 Ryan, *supra*, at 4-26. This issue is discussed below in considering liability for communicating to the public by telecommunication.

212 See CRTC Decision 86-7, as amended by Order 86-593.

213 There is some question a to whether these limitations are within the constitutional competency of the federal Parliament: see *Clark v. Canadian National Railway Co.*, [1988] S.C.R. 680 and Ryan, *supra*, at pp. 4-19 to 4-20.

The Internet provides a new challenge for ISPs, which may see themselves as "carriers" or conduits, but do not have a statutory exemption from liability.[214] Because there is no "common carrier" exemption or defence available to Canadian intermediaries on the Internet, liability of ISPs must be determined on the basis of the *Copyright Act*.

Communication by Telecommunication

The first question to determine is whether Internet intermediaries infringe the right to communicate to the public by telecommunication.

Where an intermediary performs a "carrier" function and has no role in determining or changing the content of the message which is carried, that intermediary is not communicating to the public by telecommunication. Although what an Internet intermediary transmits along its system may be a communication to the public by telecommunication (depending on the nature of the message and the recipients), the intermediary itself is not communicating to the public because it neither initiates nor receives the transmissions.

The Supreme Court of Canada recognized this fundamental distinction in *Electric Dispatch Co. v. Bell Telephone Co.*, an early telephone carrier case.[215] *Electric Despatch* involved an agreement between Bell Telephone and Electric Despatch. Prior to October 1882, Bell had operated a messenger system by which it took messages from customers over telephone lines and delivered them to others. Bell agreed to sell this business to Electric Despatch, and the contract provided that Bell "will in no manner and at no time during the term of this agreement, transmit or give directly or indirectly free or for remuneration any messenger orders to any person or persons, company or corporation". When the business which it had purchased from Bell did not live up to expectations, Electric Despatch commenced an action against Bell on the basis that third parties were using the Bell Telephone system to place messenger orders, and that Bell was therefore "transmitting such orders in breach of the contract". The Supreme Court held:

"The argument in support of [Electric

---

214 The CAIP brief to this study indicated that ISPs do not want to be considered common carriers as that term is used in the telecommunications field. They do, however, want to be viewed as a "transparent conduit".

Both the IHAC Report and the IHAC Copyright Report recommended implementation of a defence for ISPs which could demonstrate that they did not have knowledge of the infringing material and "where they have acted reasonably to limit potential abuses". Many copyright owners oppose such an exemption since they feel that it will eliminate any incentive on ISPs to monitor and remove infringing materials. See Besek, "Future Copyright Protection: Is Existing Law Adequate in a Networked World?", N.Y.L.J., December 5, 1994, at p. 1 and Axe, "Computer Bulletin Boards and Software Piracy: Are System Operators to Blame for Copyright Infringement by their Users?", *1996-97 Entertainment, Publishing and the Arts Handbook* 141 at p. 156.

215 (1891), 20 S.C.R. 83.

> Despatch's] construction of the above covenant is that when one lessee of a telephone instrument of [Bell] holds communication with another lessee of such an instrument the communication, whatever it may be, is transmitted over the wires which are the property of [Bell] from one lessee to the other, and that therefore [Bell] are the persons who "transmit" that communication, although their sole act and part in the matter is causing the wire extending from the telephone instrument of the one lessee, at the request of such lessee, to be connected with the telephone instrument of the other lessee in utter ignorance of the nature of the communication intended to be passed from one to the other, and that in case such communication should prove to be a request made upon the person receiving the communication to send a messenger to the person sending it that becomes a breach by [Bell] of their covenant. ...
>
> Doubtless the word "transmit" is an accurate expression to make use of in relation to every message which is sent from one subscriber to [Bell's] telephone exchange system to another. **Every message is transmitted from one person to another along [Bell's] wires, but in such case the person who transmits the message is no other than the sender of it. The wires constitute the mode of transmission by which one lessee transmits the message along the wires to the other. It is the person who breathes into the instrument the message which is transmitted along the wires who alone can be said to be the person who "transmits" the message. The owners of the telephone wires, who are utterly ignorant of the nature of the message intended to be sent, cannot be said within the meaning of the covenant to transmit a message of the**

> **purport of which they are ignorant.**"[216]
> (emphasis added)

In the result, Electric Despatch's claim was dismissed.

As noted earlier, there is a distinction between telephone transmissions and Internet transmissions in that some Internet transmissions involve a delay between the sending of the transmission and its eventual downloading by the recipient. At some point in the Internet transmission chain, the message is saved to a server or BBS to await its eventual retrieval by the recipient. The question is whether this makes any difference to the analysis of the potential liability of the intermediary.

Just as in *Electric Despatch*, a distinction must be made between an intermediary through whom a communication is made and the communication itself. "A communication is ordinarily considered to be a deliberate interchange of thoughts or opinions between two or more persons."[217] "A communication involves the passing of thoughts, ideas, words or information from one person to another."[218] There is a clear distinction between the person or device which activates a telecommunication facility and the facility itself.[219] This distinction does not appear to be dependent on whether the communication is instantaneous. What is important is the intention of the poster, which is to communicate with recipients. The poster has no intention of communicating with an Internet intermediary except as part of a system to complete delivery of the message.

Analogies to other copyright infringement situations also indicate that an Internet intermediary is not "communicating to the public" when it carries a user's messages. For example, outside of the broadcasting area, it has never been suggested that carriers (such as Canada Post or a trucking company) which unwittingly transport infringing copies of a copyright work are liable along with the primary infringer.[220] It would appear that the persons engaging in a "communication by telecommunication" are intended to be the initiator of the communication and its recipient. Intermediate carriers who act as a conduit have never been found to be infringing copyright in respect of information and messages which they carry in

---

216 *Electric Despatch, supra*., at pp. 90-91.

217 *Black's Law Dictionary* (6th ed., 1990), at p. 279.

218 *Goldman v. The Queen* (1979), 108 D.L.R. (3d) 17 (S.C.C.), at p. 32.

219 *R v. McLaughlin* (1980), 113 D.L.R. (3d) 386 (S.C.C.) at p. 393.

220 As discussed above, the right of "communication to the public by telecommunication" granted by Section 3(1)(f) seems to be unique in that it is the only exclusive right which is granted by the *Copyright Act* which can be accomplished through the use of an intermediary carrier such as a telephone company, cable operator or ISP. The only infringing activities which a carrier of physical goods could be seen to be involved in fall under the definition of indirect infringement in Section 27(4). For example, the delivery of a number of infringing copies by mail could be seen to be either a distribution to the public within the definition of Section 27(4)(b) or an importation under Section 27(4)(d). In both of these circumstances, a carrier such as Canada Post could not be liable since it would not in the normal course have the requisite knowledge required by Section 27(4).

either Canada or the United Kingdom and it is difficult to say logically that they are communicating with anyone.[221]

This issue was recently considered in the United States in the *Netcom* decision. *Netcom* is one of several actions worldwide being pursued by the Church of Scientology through Religious Technology Center (RTC) and other corporations in an attempt to keep Scientology's secret documents from being transmitted over the Internet.[222] In the *Netcom* case, a former Scientology member, Dennis Erlich, had posted several secret Scientology documents to a Usenet group called "alt.religion.scientology". This newsgroup was maintained by Tom Klemesrud, who in turn contracted with Netcom to provide Internet access through its facilities.

The facts in *Netcom* were not seriously in dispute, and it was not contested that the posting by Erlich of the Scientology documents was an infringement of the RTC copyright. Immediately after the Erlich postings, RTC had sent written notice to both Klemesrud and Netcom claiming that the Erlich postings were a copyright infringement. Klemesrud and Netcom permitted the postings to remain available on the Internet for 11 days after RTC sent its notice. RTC commenced a copyright infringement action against Erlich, Klemesrud and Netcom.

Both Klemesrud and Netcom brought summary judgment motions seeking dismissal of the claims against them. Whyte, J. granted summary judgment dismissing RTC's direct and vicarious infringement claims, but permitting the claims based on contributory infringement to proceed to trial. Although specific to American copyright law, some of the logic of the *Netcom* decision is compelling, particularly in respect of the direct infringement claims.

In considering the direct infringement claim against Klemesrud and Netcom, Whyte, J. first noted that, unlike large on-line service providers like Compuserve, America On-line and Prodigy, "Netcom does not create or control the content of the information available to its subscribers". Netcom admitted, however, that it had the technology to screen messages containing particular words or originating from particular individuals, although Netcom had

---

221 The only other common situation in which a carrier of telecommunications is liable for copyright infringement is that of cable operators delivering television and radio signals to customers. Cable operators do not, however, simply pass along the signals; they alter them as well. As a result, what is sent to the cable operator's customers is not the communication which was received by the operator, but a wholly new communication. This would make the cable operator the originator of a new "communication to the public by telecommunication".

In the *CCTA* case, there does not appear to have been any argument concerning whether the cable operators were "communicating by telecommunication". Rather, the decision focused on the definition of "musical work" and the Federal Court of Appeal appears to have assumed that the cable operators were in fact were communicating by telecommunication.

222 One of several Web sites devoted to coverage of the various Scientology Internet actions is http://www.cybercom.net/~rnewman/scientology/home.html.

declined to consider such an alternative when RTC's notice had been received. These comments again emphasize that the role played by an Internet intermediary in specific Internet transmissions will be of critical importance in determining its potential liability.[223]

After finding (based on *MAI v. Peak*[224]) that fixed copies of the RTC copyright material had been made by Klemesrud and Netcom, Whyte, J. then considered the potential liability of Klemesrud and Netcom for such infringement:

> "Accepting that copies were made, Netcom argues that Erlich, and not Netcom, is directly liable for the copying. *MAI* did not address the question raised in this case: whether possessors of computers are liable for incidental copies automatically made on their computers using their software as part of a process initiated by a third party. Netcom correctly distinguishes *MAI* on the ground that Netcom did not take any affirmative action that directly resulted in copying plaintiffs' works other than by installing and maintaining a system whereby software automatically forwards messages received from subscribers on to the Usenet, and temporarily stores copies on its system. Netcom's actions, to the extent that they created a copy of the plaintiffs' works, were necessary to having a working system for transmitting Usenet postings to and from the Internet. Unlike the defendant in *MAI*, neither Netcom nor Klemesrud initiated the copying. ... Netcom's and Klemesrud's systems can operate without any human intervention. Thus, unlike *MAI*, the mere fact that Netcom's system incidentally makes temporary copies of plaintiffs' works does not mean that Netcom has caused the copying. **The court believes that Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of owner of a copying machine who lets the public make copies with it. Although some of the people using the machine may directly infringe copyrights, courts analyze the machine owner's liability under the rubric of contributory infringement, not direct infringement.** ...

---

223 While Whyte, J. contrasted Netcom's role to that of Compuserve and the other large on-line services, there is nothing in the judgment which would indicate that there is anything special about such services which would in itself expose them to increased liability. Rather, the court was distinguishing between a service's function as a carrier or conduit and its function as a content provider. There is no reason to believe that Whyte, J. would have found Compuserve liable had Erlich posted the Scientology material to one of Compuserve's libraries or forums without Compuserve's consent.

224 (1993), 991 F. 2d 511.

> Plaintiffs' theory would create many separate acts of infringement and, carried to its natural extreme, would lead to unreasonable liability. It is not difficult to conclude that Erlich infringes by copying a protected work on to his computer and by posting a message to a newsgroup. However, plaintiffs' theory further implicates a Usenet server that carries Erlich's message to other servers regardless of whether that server acts without any human intervention beyond the initial setting up of the system. It would also result in liability for every single Usenet server in the worldwide link of computers transmitting Erlich's message to every other computer. These parties, who are liable under plaintiffs' theory, do no more than operate or implement a system that is essential if Usenet messages are to be widely distributed. There is no need to construe the [Copyright] Act to make all of these parties infringers. Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party. ...
>
> [The storage on a defendant's system of infringing copies and retransmission to other servers is not a direct infringement by the BBS operator of the exclusive right to reproduce the work where such copies are uploaded by an infringing user. ...
>
> The court is not entirely convinced that the mere possession of a digital copy on a BBS that is accessible to some members of the public constitutes direct infringement by the BBS operator. Such a holding suffers from the same problem of causation as the reproduction argument. **Only the subscriber should be liable for causing the distribution of plaintiffs' work as the contributing actions of the BBS provider are automatic and indiscriminate.** Erlich could have posted his messages through countless access providers and the outcome would be the same: anyone with access to Usenet newsgroups would be able to read his messages. There is no logical reason to draw a line around Netcom and Klemesrud and say that they are uniquely responsible for distributing Erlich's messages. Netcom is not even the first link in the chain of distribution - Erlich had no direct relationship with Netcom but dealt solely with Klemesrud's BBS, which used Netcom to gain its Internet access. Every Usenet server has a role in the distribution, so plaintiffs' argument would create unreasonable liability. **Where the BBS merely stores and passes along all**

> **messages sent by its subscribers and others, the BBS should not be seen as causing these works to be publicly distributed or displayed. ...**
>
> The court is not persuaded by plaintiffs' argument that Netcom is directly liable for the copies that are made and stored on its computer. **Where the infringing subscriber is clearly directly liable for the same act, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet. Such a result is unnecessary as there is already a party directly liable for causing the copies to be made. ...** The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred. Billions of bits of data float through the Internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from noninfringing bits. Because the court cannot see any meaningful distinction between what Netcom did and what every other Usenet server does, the court finds that Netcom cannot be held liable for direct infringement."[225] (emphasis added)

While Whyte, J.'s comparison of Netcom's role to that of a photocopier owner may not be completely apt, his decision to determine Netcom's potential liability on the basis of contributory infringement, rather than direct infringement, is important. Contributory infringement has no direct analogy under Canadian copyright law, but shares some characteristics with the concept of "authorization" and indirect infringement. As discussed above, Canadian law has never held the owners of equipment such as photocopiers to be liable for infringements by third parties using the equipment.[226]

By confirming that the liability of passive Internet intermediaries like Klemesrud and Netcom is to be determined only on contributory infringement grounds, the decision in

---

225 *Netcom*, at pp. 7-14.

226 "Liability for participation in the infringement will be established where the defendant, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.": *Netcom*, at p. 15, citing *Gershwin Publishing Corp. v. Columbia Artists Mgmt. Inc.* (1971), 443 F. 2d 1159. It is clear that "authorization" under Canadian copyright law is narrower than the American concept of contributory infringement, and the knowledge requirement makes it similar to indirect infringement under Section 27(4). Potential liability of Internet intermediaries for both authorizing copyright infringement and indirect infringement is discussed later in this report.

Netcom confirms that the copies of RTC's copyright works were being made by the user Erlich using the intermediaries' equipment and systems, and not by the intermediaries themselves. As a result, there is no direct infringement by those intermediaries.[227]

The logic of the *Netcom* decision on the issue of liability of Internet intermediaries for direct copyright infringement comes from the policy considerations stated by Whyte, J. Clearly, if a theory of liability would cast a net so wide as to be patently unreasonable, there must be something amiss with the theory.

It would appear, therefore, that many Internet intermediaries are not communicating by telecommunication when they transmit the messages of their users. It must be recognized, however, that intermediary liability must be examined based on the facts of each Internet communication and the role played by each intermediary in each such communication. If the intermediary has an active role in the specific communication, then it may be possible that it is communicating by telecommunication along with its user. In the case of most commercial ISPs, whose role in communications to or from its users tends to be closer to a carrier than a poster or a recipient, it may be relatively rare that they will be communicating by telecommunication when their users send infringing copies of works.

Section 3(1.3) of the *Copyright Act* and Intermediary Liability

In discussions of the liability of Canadian intermediaries on the Internet, much attention has been focused on the exemption contained in Section 3(1.3) of the *Copyright Act*. It must be recognized, however, that the exemption in Section 3(1.3) is a rather narrow one. Section 3(1.3) provides as follows:

> "(1.3) *Restriction.* - For the purpose of paragraph (1)(f), a person whose only act in respect of the communication of a work to the public consists of providing the means of telecommunication necessary for another person to so communicate the work does not communicate that work to the public."

The exemption in Section 3(1.3) only applies to infringements of the right to communicate to the public by telecommunication. If the conditions set out in Section 3(1.3) are met, then the person is deemed to not be communicating to the public by telecommunication. If an ISP is infringing any of the other rights granted by the *Copyright Act*, however, Section 3(1.3) may not provide an exemption from liability for infringement.

---

227 "Without evidence of the operator's direct involvement in the uploading and downloading of copyrighted material, a direct infringement analysis is inappropriate.": Dobbins, "Computer Bulletin Board Liability for Users' Infringing Acts", 191 Michigan Law Review 217 (1994), at p. 222.

Even if an Internet intermediary were to be seen as "communicating to the public by telecommunication" when it transmits infringing messages on the Internet over its system, such an intermediary will be deemed by Section 3(1.3) not to be so communicating if its "only act in respect of the communication of a work to the public consists of providing the means of telecommunication necessary for another person to so communicate the work". This provision would clearly exempt a telecommunications carrier or other entity which forms part of the Internet "backbone" from any liability for communicating an unauthorized copyright work to the public over its system. If the carrier makes no reproduction of the work during the course of its carriage of the communication of the work, it should have no potential copyright infringement liability whatsoever.

The more difficult question concerns whether ISPs, on-line services and BBS sysops can rely on Section 3(1.3), and in what circumstances. ISPs often perform a true "carrier" role in Internet transmissions. One difficulty arises when, in the process of "providing the means of telecommunication", the ISP also infringes on one of the other exclusive rights of the copyright owner. As noted above, ISPs may reproduce copyright works in the course of transmitting e-mail messages (which are retained on an ISP's mail server), facilitating Web browsing (where unauthorized copyright Web page elements are cached by an ISP) and permitting newsgroup access (where an infringing copy of a work may reside on an ISP's news server).[228] In each of these cases, the ISP is "providing the means of telecommunication", but in doing so may have infringed on another exclusive right of the copyright owner. The issue then arises as to whether the Section 3(1.3) exemption is still available.

The Supreme Court of Canada made it clear in *Télé-Métropole*[229] that an infringement of one of the exclusive rights of a copyright owner is nevertheless an infringement even if it occurs in the course of the exercise of a licensed use of another of the exclusive rights . As a result, a reproduction made by an ISP for the purpose of caching or mirroring may still be an unauthorized reproduction even if the poster of the work had obtained a license to communicate the work to the public by telecommunication.

It should follow that the converse is also true. Even if an infringement of one of the other exclusive rights granted by the *Copyright Act* takes place during the course of an ISP "providing the means of telecommunication necessary" for the transmission to be made, the exemption contained in Section 3(1.3) should still be available to preclude the ISP from liability for communicating the work by telecommunication.[230] The question is whether the caching done by the ISP was in fact part of "providing the means of telecommunication necessary" to the transmission.

---

228 The issue of whether the ISP is responsible for the infringement of the reproduction right is discussed below.

229 [1990] 2 S.C.R. 467.

230 As will be discussed further below, this distinction is important in determining whether certain rights have been infringed and royalties are therefore payable.

The critical words in interpreting the application of Section 3(1.3) are “only act” and “necessary”. The role of the intermediary in respect of a particular communication of a particular work must be examined in order to determine whether that intermediary's “only act” is providing the means of telecommunication “necessary” to complete the communication.

In respect of the words “only act”, it must be noted that Section 3(1.3) deals quite specifically with individual communications of a work. Internet intermediaries which provide services in addition to acting as a conduit for communications are not necessarily excluded from reliance on Section 3(1.3); their role in each infringing communication must be examined more or less in isolation. Therefore any analysis of whether an ISP’s “only act” was providing the means of telecommunication must be done solely in the context of the specific infringement which is being alleged.[231]

The meaning of the word “necessary” in Section 3(1.3) is somewhat ambiguous. It is possible to argue that, even in respect of individual Internet transmissions, ISPs will perform tasks which are not strictly necessary. An example is caching, which, although it improves the efficiency of Internet transmissions, is not strictly "necessary". If the word “necessary” in Section 3(1.3) was interpreted to mean that any unnecessary step or procedure which is taken by an Internet intermediary precludes reliance on Section 3(1.3), it is unlikely that this exemption could be relied on at all.[232]

The better view of the interpretation of Section 3(1.3) would seem to be that “necessary” refers to the relationship generally between the “means” and the “communication”, and only requires that what the ISP is doing in respect of the individual communication in question be part of the general manner in which the ISP provides the means by which communications are transmitted. As a result, an ISP could rely on Section 3(1.3) and would not be “communicating to the public by telecommunication” when it acted as a conduit for Internet transmissions to and from its customers.

Intermediaries and Authorization

There is a wide range of intermediary involvement in the Internet communications chain. Some intermediaries permit the use of their equipment and systems by posters and recipients solely to facilitate their communications. Some intermediaries do not impose any control whatsoever over the postings to their systems, others moderate newsgroups and

---

231 Thus, for example, the fact that are ISP also created and communicated other works as a poster rather than a conduit should have no effect on the ability of the ISP to resort to Section 3(1.3) in respect of the specific acts at issue.

232 An interpretation that the means employed by an intermediary must be “necessary” to any particular transmission in order to invoke the application of Section 3(1.3) leaves open pure telecommunications carriers such as telephone companies to copyright claims if their system includes any process which is not strictly essential to the Internet transmission in question. This clearly is not the intent of Section 3(1.3).

discussion groups, and some take active steps to control content by editing or censoring postings. It may be that the extent of the involvement of a BBS in the activities of its users and the content of postings will be a major determinant of its potential liability.[233]

As has been discussed above, Canadian case law has made it clear that the provision of equipment which is used to infringe copyright is not an "authorization" such as to make the owner of the equipment liable along with the primary infringer. ISPs and BBS sysops whose equipment is employed by users to infringe copyright do not by that fact alone have any liability for direct copyright infringement. Therefore, even if a user causes an ISP's equipment to make an infringing reproduction or an unauthorized communication by telecommunication, the ISP does not in the normal course become a joint infringer with the user.

Whether such intermediaries could be seen to be authorizing a communication to the public by telecommunication when users post unauthorized copyright material on the systems of the intermediaries will depend on the proper analysis of all of the circumstances in each individual case. In some situations, the activities of the intermediary will be such that the intermediary is personally participating in an infringing communication. For example, if a BBS sysop were to post a message on an Internet newsgroup requesting posters to copy pictures from *Playboy* on to his server so that other BBS users could download such images, then it would be likely that the BBS sysop would be personally liable for communicating those works to the public by telecommunication when users downloaded the images to their computers. The sysop in such a situation is acting in concert with others, is supplying the means by which third parties are infringing copyright and has full knowledge of the infringing activities.[234]

---

233 "If there is room for liability of the provider who runs a BBS, it is very much dependent on the measure in which he commits himself to the content of the information.": Kasperson, "Liability of Providers of the Electronic Highway", [1996] 12 C.L.S.R. 290.

234 The sysop in this case would be in the position of the restaurant owner in *Vigneux v. Canadian Performing Right Society*, [1945] A.C. 106 (P.C.). This appears to have been the basis for liability in *Playboy Enterprises, Inc. v. Frena* (1993), 839 F. Supp. 4552 (U.S.D.C. Fla.) and *Sega Enterprises, Inc. v. Maphia* (1994), 857 F. Supp. 679 (U.S.D.C. Cal.). In the *Sega* case, the BBS sysop was found to have provided downloading privileges for unauthorized copies of Sega games in exchange for either goods or services or the uploading by users of other games by Sega and other manufacturers. This decision has been criticized as casting too wide a net over BBS sysops:

> "Although a BBS as a communications facility arguably provides users with the means for copying information, nothing in the BBS operation itself facilitates the infringement. The infringing nature of this "uploading" and "downloading" activity stems from the fact that some information on the BBS might be copyrighted material, and may not be licensed for certain uses. Imposing liability upon BBS operators for merely providing the facility on which copyright infringement may take place establishes an extensive liability rule."

Elkin-Koren, "Copyright Law and Social Dialogue on the Information Superhighway", 13 Cardozo Arts

At the other end of the spectrum is the on-line service which sets up a number of forums or other areas which are operated by independent contractors which have complete control over content.[235] If a user infringes copyright by employing the on-line service to communicate an infringing copyright work to the public by telecommunication, it would appear anomalous that the intermediary (which has no knowledge of an individual infringement and no practical way of either monitoring the traffic through its system or screening infringing communications) would be strictly liable for copyright infringements which take place. The on-line service has had no direct involvement with the infringement and, although its equipment and systems may have facilitated the infringement by the user, under Canadian copyright law that is not an authorization of the infringement.

In *Netcom*, the Court decided that the contributory infringement claim by RTC against Klemesrud and Netcom should proceed to trial because there was an issue of fact concerning "whether Netcom knew of any infringement by Erlich before it was too late to do anything about it."[236] The Court found:

> "Thus, it is fair, assuming Netcom is able to take simple measures to prevent further damage to plaintiffs' copyrighted works, to hold Netcom liable for contributory infringement where Netcom has knowledge of Erlich's infringing postings yet continues to aid in the accomplishment of Erlich's purpose of publicly distributing the postings."[237]

Although this appears to be a correct statement of the test for contributory infringement under United States copyright law, it is not clear that the same result would be reached in Canada. There has been no case in Canada where a person's knowledge of an infringement, combined with an ability of that person to take "simple measures" to prevent its continuation, created liability for copyright infringement. In fact, the decision in *Apple Computer*[238] held that there was no liability in such an instance. In that case, a person who was knowingly financing the infringing activity (and as a result would seem to have been in a position to take "simple measures" to stop the infringement) was not liable since he had not authorized the infringement. In certain circumstances, such a person could be guilty of indirect infringement, as is discussed in the following section.

At some point, however, the actions of an Internet intermediary could change from that of an independent service provider to that of a direct participant in the infringement. The

---

and Entertainment L.J. 346 (1995).

235 This was found to be the factual nexus in *Cubby v. Compuserve, Inc.* (1991), 776 F. Supp. 135 (N.Y.), a defamation case. All of the major on-line services operate in similar manner, although some exercise more direct control over some or all of the content on their systems.

236 *Netcom*, p. 16.

237 *Netcom*, p. 18.

238 *Apple Computer, Inc. v. Mackintosh Computers Ltd.* (1986), 28 D.L.R. (4th) 178 (F.C.T.D).

demarcation line is not clear, but neither knowledge nor the ability to prevent the infringement seem to be sufficient under Canadian law. As a result, it would appear that most Internet intermediaries would not be considered to be authorizing infringement by their users.

Other Intermediary Liability

As noted above, there is an infringement of the reproduction right any time caching is done in Canada of unauthorized copyright works. There is also an infringement of the reproduction right when e-mail messages and newsgroup postings are saved to servers of the ISP of the poster, recipient or newsgroup. The issue is who is responsible for the infringement, the poster, the ISP or both? There appears to be little doubt that the poster is liable even though the reproduction may have been made using the equipment belonging to the ISP. However, as has been discussed above, an ISP should not be liable for direct infringement in a situation where the poster has caused the reproduction on the ISP's equipment without any involvement or knowledge of the ISP.

A determination of the ISP's liability for infringement of the reproduction right likely would depend on whether the ISP is making the decision to reproduce the work or whether it is the user which is reproducing the work using the ISP's equipment. In the former case, the ISP is unquestionably liable; in the latter case, the ISP does not appear to be either personally infringing or authorizing infringement, and, absent any knowledge of the infringing reproduction, the ISP should not be liable for an infringement of the reproduction right.

There may be a distinction between "blind" caching by an ISP and advertent caching of popular Web sites. In *Netcom,* the court emphasized both that Netcom had done nothing more than what was necessary to ensure operation of the Usenet system and that the reproduction of the works by Netcom was automatic and involved no human intervention.[239] The decision might have been different if Netcom had decided to make additional copies of the works in issue and made them available in order to speed access for its subscribers.

Similar consideration apply to BBS sysops and on-line services. In many cases, and in particular in respect of the major on-line services, the BBS or on-line service is merely providing equipment which is then employed by the users to reproduce infringing copies of copyright works. Under Canadian law, this is not authorizing copyright infringement even if it does facilitate such infringement.[240]

One common difficulty arises when an ISP or other intermediary is given notice that

---

239 *Netcom*, at p. 9.

240 "In circumstances where the owner of the bulletin board cannot be shown to have placed the allegedly infringing item on her own computer, it may be difficult to show that the bulletin board operator has infringed the reproduction right, because - at least until the point of transmission to the requester - the bulletin board operator has not herself caused a copy to be made.": Perritt, "Law and the Information Superhighway" (1996), at p. 430.

a user is infringing copyright or that there might be infringing material on the intermediary's servers or system. In *Netcom*, the court found that Netcom might be liable as a contributory infringer because, having received notice from the owner of the copyright that infringement might be occurring, Netcom failed to take any steps for 11 days to stop the infringement. The court held that an ISP would not be expected to act on a mere allegation but, having received reasonable notice, the service provider would at some point be expected to cut off an infringing subscriber's access.[241]

Canadian copyright law does not recognize the concept of "contributory infringement", and the issue in a similar case in Canada would be whether the ISP had sufficient knowledge of the infringement to either qualify as a joint infringer or be guilty of indirect infringement pursuant to Section 27(4). A sysop in such cases could be guilty of indirect infringement if it could be shown that the sysop had knowledge of the infringing nature of the activities, and that the activities were such as to fall within one of the categories enumerated in Section 27(4). For example, the sysop might be seen to be distributing the work, either "for the purposes of trade" or "to such an extent as to affect prejudicially the owner of the copyright", if the sysop did not take reasonable steps to stop continued transmissions after obtaining knowledge of the copyright infringement.[242]

The issue of notice and knowledge is a difficult one. In many cases, an ISP is presented with a claim by a person that it owns copyright material and that there are infringing copies on the ISP's system. The ISP has no practical way in which to determine whether the claimant actually owns the copyright in the material (or the specific rights which are claimed to be infringed), and there may be allegations that the claimant has licensed the use of the material. If the ISP removes the material from its system, it may be unjustifiably interfering with its user's privacy and property if the claim of copyright infringement is not valid; if the ISP refuses to remove the material in the absence of positive proof of the claimant's rights, it may face a claim by the claimant that the ISP has infringed the copyright in the material.

The Code of Conduct which has recently been issued by the Canadian Association of Internet Providers (CAIP) attempts to deal with this conundrum by giving ISPs some guidelines on how to resolve disputes over rights.[243] It appears, however, that the Code is so general that it provides no practical solution to an ISP faced with a claim that one of its users is infringing copyright.

It is possible to summarize this analysis of intermediary liability as follows:

a) whether an Internet intermediary communicates

---

241 *Netcom*, pp. 14-22; Cameron and Onyshko, "Intellectual Property and the Internet", paper available at http://www. jurisdiction.com.

242 As discussed above, it is unclear whether the concept of "distribution" applies to digital copies transmitted over the Internet.

243 See "Internet group strikes conduct code", *Globe & Mail*, November 2, 1996, p. B3.

copyright works to the public by telecommunication will depend on the circumstances of the specific infringing communication. If the intermediary does not participate in the infringing activity, then the intermediary is not communicating to the public by telecommunication. The intermediary would in any event likely be exempted by Section 3(1.3);

b) where an intermediary's equipment and systems are being used by others to infringe, the intermediary will not be liable for authorizing copyright infringement if its equipment and systems have a significant non-infringing use and the intermediary does not "do something more" than encourage or facilitate the infringing activity;

c) where an Internet intermediary reproduces copyright works as part of its transmission system, in particular by caching Web pages which contains such works, the intermediary might be liable for infringing the reproduction right, although there should be no liability for temporary reproductions made "automatically and uniformly" on the intermediary's equipment as part of the overall Internet transmission system;

d) where an intermediary is a knowing participant in copyright infringement, either intentionally or through "willful blindness" after being provided with reliable evidence of infringing activities, the intermediary may be liable for indirect infringement pursuant to Section 27(4) if the work is distributed or if the other conditions in that provision are met.

As a last word on intermediary liability, it must be noted that the limits of such liability will, in the final analysis, be decided by courts or legislators based on a balancing of the interests of the intermediaries and the copyright owners.[244] While there is little in copyright law which would logically make an ISP liable for infringement each time one of its users transmits an infringing copy of a work over the Internet, it is argued that imposing some liability on the ISP is required in order to "enlist" their support in preventing widespread

---

244 See Loundy, "Revising the Copyright Law for Electronic Publishing", 14 J. of Comp. & Info. Law 1 (1995) for a discussion of the need for a balanced view.

infringement.[245] The difficulty with this approach is that it may unfairly penalize intermediaries and discourage investment in the Internet. As is discussed below, there are alternative methods to control copyright infringement, including technological advances which will permit digital copies of works to be marked and royalties collected automatically. Some authors see a combination of collectivization of royalties and imposition of liability on Internet intermediaries as the only alternatives to ensure remuneration for use of copyright material reaches copyright owners.[246] Others try to justify a policy of strict liability for Internet intermediaries on economic grounds.[247] Courts and legislators should be hesitant to bend

---

245 "We probably want to enlist the system operators, as we have enlisted libraries and employers, to help educate their users about the copyright laws, and to set up a reasonable system for policing against infringing activities. And perhaps the only effective means for inducing their cooperation is to hold them liable for copyright infringement if they fail to provide adequate safeguards against infringing activity, or at least infringing activity of which they have knowledge."

Slotnick, "Copyright Concerns on the Information Superhighway", *1994 Annual Survey of American Law* 383, at p. 391.

246 Ginsburg, "Putting Cars on the "Information Superhighway": Authors, Exploiters and Copyright in Cyberspace", 95 Columbia L. Rev. 1466 (1995), at pp. 1488-1489. The author correctly points out that infringement enforcement has historically been concentrated "higher up the chain of distribution" because "pursuing the intermediary offered the most effective way to enforce copyright interests". It is clear that most Internet intermediaries (such as ISPs and on-line services) are not intermediaries of the type cited (publishers and producers of movies and records). The latter are intermediaries in that they assemble content as part of a top-down distribution system; Internet intermediaries tend to be closer to transporters of content created or assembled by others and provided to them as a finished product to be communicated. The author's further analogy to theatres where copyright works are performed is also inapposite, at least in Canada. Section 27(5) specifically makes theatres and "other places of entertainment" liable if infringing performances are held; there is no similar provision relating to the Internet; see also *de Tervagne v. Beloeil* (1993), 50 C.P.R. (3d) 419 (F.C.T.D.).

The submissions to this study by several content owners recommended that strict liability be imposed against Internet intermediaries, even though some suggested that individual licensing of copyright works on a per work or transaction basis is feasible. It is unclear why intermediaries should be strictly liable for any infringement if the ultimate user can be charged directly for the use of the copyright work. At least one creator group opposed liability being imposed on ISPs unless the ISP had actually uploaded the infringing material.

247 Hardy, "The Proper Legal Regime for 'Cyberspace'", 55 U. of Pitt. L. Rev. 995 (1994), at pp. 1041-1048. The author argues that "strict liability will force the system administrator of each BBS service to determine the most advantageous mix of preventative measures for that BBS". In essence, strict liability will force the Internet intermediary either to insure for someone else's liability or to screen its subscribers for solvency in case the intermediary need to commence an indemnity action against the subscriber. As was pointed out in *Netcom*, an Internet intermediary may have no relationship whatsoever with the primary infringer and may not even be able to locate them. All that imposing strict copyright infringement liability on intermediaries will do is increase their cost of doing business, whether as a result of increased insurance costs or from having to pay damages to copyright owners, which in turn passes along the costs of infringement onto all other users. In effect, the majority of "good" users will subsidize the infringement of the "bad" users. There will be no incentive on "bad" users to stop infringing, since copyright owners will rarely, if ever, take action against an individual user if a convenient intermediary is available.

The imposition of strict liability on Internet intermediaries would be easier to justify if there were to be

copyright principles too far solely to recruit Internet intermediaries to the cause of preventing copyright infringement by their users.

(e) Tariff 22

In September, 1995, SOCAN published the first tariff intended to claim royalties for music use on the Internet. The tariff provides a license:

> "to communicate to the public by telecommunication, in Canada, musical works forming part of SOCAN's repertoire, by a telecommunications service to subscribers by means of one or more computer(s) or other device that is connected to a telecommunications network where the transmission of those works can be accessed by each subscriber independently of any other person having access to the service".

The licensee is required to pay a monthly fee calculated as follows:

> "(a) in the case of those telecommunications services that do not earn revenue from advertisements on the service, $0.25 per subscriber; and
>
> (b) in the case of those telecommunications services that earn revenue from advertisements on the service, 3.2 per cent of gross revenues, with a minimum fee of $0.25 per subscriber".

The various terms used in Tariff 22 as defined follows:

> "Telecommunications service" includes a service known as a computer on-line service, an electronic bulletin board service (BBS), a network server or service provider or similar operation that provides for or authorizes the

---

collectivization of royalty payments for all copyright material such that intermediaries can be assured that there is a fair allocation of responsibility for royalties which can then be passed on to users in a just way. It seems unlikely, absent international agreement, that such collectivization could realistically be accomplished on the Internet in the near future.

> digital encoding, random access and/or storage of musical works or portions of musical works in a digitally encoded form for the transmission of those musical works in digital form via a telecommunications network or that provides access to such a telecommunications network to a subscriber's computer or other device that allows the transmission of material to be accessed by each subscriber independently of any other person having access to the service. "Telecommunications service" shall not include a "music supplier" covered under Tariff 16 or a "transmitter" covered under Tariff 17.
>
> "Subscriber" means a person who accesses or is contractually entitled to access the service provided by the telecommunication service in a given month.
>
> "Gross revenues" includes the total of all amounts paid by subscribers for the right to access the transmissions of musical works and all amounts paid for the preparation, storage or transmission of advertisements on the service.
>
> "Advertisements on the service" includes any sponsorship announcement, trade-mark, commercial message or advertisements displayed, communicated or accessible during connection to or with the service or to which the subscriber's attention is directly or indirectly guided by means of a hypertext link or other means.

SOCAN controls the "public performance" right and the "communication to the public by telecommunication" right for most musical works in Canada. Tariff 22 does not refer to a license for public performance rights and it must be assumed that SOCAN is of the view that Internet transmissions are communications to the public by telecommunication.

In the *Télé-Métropole* case, the Supreme Court of Canada held that SOCAN's predecessor could not license the making of a reproduction, and the fact that a broadcaster held a public performance license did not permit a reproduction of a work in the course of

exercising the public performance right.[248] In other words, each of the exclusive rights granted by the *Copyright Act* is separate and distinct; the licensing of one does not permit the exploitation of another right by the licensee. As a result, if Internet intermediaries are not infringing the right to communicate to the public by telecommunication, then, even if these intermediaries are infringing other rights such as the reproduction right, there may be no basis for seeking royalty payments from them.[249]

As can be seen from the discussion in this study, Canadian copyright law tends to focus on specific activities rather than categories of users. Tariff 22 differs from some of SOCAN's other tariffs in that it describes who is liable to pay the specified royalty ("telecommunications services") and the media through which the communication to the public is accomplished ("by means of one or more computer(s) or other device that is connected to a telecommunications network where the transmission of those works can be accessed by each subscriber independently of any other person having access to the service"), but does not describe the infringing acts which are claimed to be the basis of the tariff. As drafted, Tariff 22 therefore leaves open the issue of the nature of the acts for which the telecommunications services are expected to pay to SOCAN the specified royalties.

The various issues discussed in this study in relation to the liability of Internet intermediaries will likely have a bearing on the Copyright Board's consideration of Tariff 22. The Board will have to consider whether, and in what circumstances, the intermediaries which SOCAN has named in Tariff 22 have liability for communicating copyright works to the public by telecommunication. If the Board determines that the intermediaries are in fact communicating copyright works to the public by telecommunication, the Board will also have to consider the extent of that infringement in order to consider whether the quantum of the

---

248 [1990] 2 S.C.R. 467 at pp. 485-487.

249 In its submissions to the study, SOCAN agreed that a distinction had to be made between an infringement of the reproduction right and an infringement of the right to communicate to the public by telecommunication.

royalty requested by SOCAN is appropriate.[250] The Board may also have to consider whether intermediaries which are located outside of Canada are communicating to the public in Canada when their transmissions are received by Canadians.

Because Tariff 22 is presently before the Copyright Board, it would be inappropriate for this study to comment further on the specifics of the tariff or the positions which have been, or might be, taken by the participants. Clearly, however, the issues before the Board are of great interest to copyright owners and users generally.[251]

(f) Defences to Internet Copyright Infringement

(i) Fair dealing and other exemptions

The fair dealing exceptions are set out in Sections 27(2)(a) and (a.1) of the *Copyright Act*:

> 27(2) The following acts do not constitute an infringement of copyright:
>
> (a) any fair dealing with any work for the purposes of private study or research;
>
> (a.1) any fair dealing with any work for the purposes of criticism, review or newspaper summary, if (i) the source, and (ii) the author's name, if given in the source, are mentioned.

---

250 There do not appear to be any statistics which indicate how much of the traffic over the Internet actually contains material over which copyright could or would be claimed. None of the submissions to this study were able to provide any such information, although the Educational Media Producers and Distributors Association of Canada (EMPDAC) stated in their submission that "the majority of works on the Internet are copyright". SOCAN has indicated to the Copyright Board that it intends to present such evidence in respect of Tariff 22.

Speculation by commentators about the proportion of Internet transmissions which are subject to copyright ranges widely. "The amount of information available over electronic media is phenomenal and is growing at an incredible rate. Much of the information is in the public domain because the author does not claim a copyright or one has expired": Meyer, "National and International Copyright Liability for Electronic System Operators", available at http://law.indiana.edu/glsj/vol2/no2/meyer.html; "There are literally hundreds of locations on the Internet ... where digitized music can either be given away or acquired for free - without the copyright owners' permission." Segal, "Dissemination of Digitized Music on the Internet: A Challenge to the Copyright Act", 12 Santa Clara Comp. & High Tech. L.J. 97 (1995), at p. 100. Neither view appears to have much empirical support.

251 See Hayes, "Tollbooth on the Information Highway? Canada's Music Collective Looks for Royalties on the 'Net", 1-5 *Cyberspace Lawyer* 11 (1996).

As can be seen, Section 27(2) provides quite specific exemptions for "fair dealing". This is to be contrasted to Section 107 of the *United States Copyright Act* which provides an exception for "fair use" of a copyrighted work. The definition of fair use is relatively open ended and depends on the nature and purpose of the use and "the effect of the use upon the potential market for or value of the copyrighted work".[252]

There are relatively few Canadian cases on the fair dealing exemption, but it is fair to say that the scope of the exemption has been found to be quite narrow. There can be no fair dealing where the entire work is reproduced.[253] In some instances, even quite small takings from a copyright work have been held not to be fair dealing.[254]

The basic rationale of fair dealing is to permit limited private use or quotation of a copyright work provided that such use does not compete with the interests of the copyright owner.[255] Ultimately, it is a matter of impression.[256]

Some Internet communication of copyright works could be seen as fair dealing. For example, if a newsgroup or Web site were devoted to discussion of the work of a musician or author, it is possible that limited extracts from copyright works by or relating to the newsgroup's subject could be posted under the fair dealing exemption.

Very substantial amendments to the fair dealing exemption are proposed in Bill C-32. The fair dealing exemption in respect of research, private study, criticism or review is continued[257] and a fair dealing exemption for news reporting or news summary has been added.[258] None of these amendments would appear to have any significant effect on Internet copyright infringement liability.

Section 27 also contains a number of specific exemptions relating to schools, archival deposits and backup copies of computer programs. Bill C-32 proposes to substantially amend these exemptions.[259] It is beyond the scope of this study to analyze the specifics of either the current exemptions or the Bill C-32 proposals, but it is clear that the proposed amendments to the *Copyright Act* significantly extend the available exemptions,

---

252 Knopf, "Limits On the Nature and Scope of Copyright" in Henderson, "*Copyright Law of Canada*" (1994), at pp. 256-259; Wolfson, "Information Providers on the Information Superhighway - Liability Issue", in Kyer and Erickson, *CLA Computer Law Companion III*, at pp. 311-318; *Netcom*, at pp. 23-27.

253 *Zamacois v. Douville* (1943), 2 C.P.R. 270 (Ex. Ct.).

254 *Breen v. Hancock House Publishers Ltd.* (1985), 6 C.P.R. (3d) 433 (F.C.T.D.), at p. 436.

255 Laddie, *The Modern Law of Copyright* (1980), at ¤2.110.

256 *New Era Publications Int., ApS v. Key-Porter Books Ltd.* (1987), 18 C.P.R. (3d) 562 (F.C.T.D.), at p. 568.

257 Sections 29 and 29.1.

258 Section 29.2.

259 Sections 29.3 through 32.3.

especially for educational institutions.[260] For example, the amended provisions will likely permit use of Internet downloads in the classroom without liability for infringing the copyright in any of the works contained in those transmissions.

(ii) Implied license

Where a copyright owner deals with the work, or authorizes others to deal with the work, in such a way that it invites others to make use of the work in a certain way, it can be said that the copyright owner has given an implied consent or license to such use, even if there is no specific license given to any individual user.[261] Even though Section 13(4) of the *Copyright Act* requires that any assignment or grant of an interest in a copyright must be in writing, an implied license will be created where the nature of the transaction makes it necessary to do so.[262] The onus would likely be on the defendant which is alleging the existence of an implied license to prove both the fact of the license and its operative terms.[263]

This concept of implied licenses is important to the question of the caching done by ISPs when their users download Web pages. If the copyright owner has permitted the work to be placed on the Web, it can be argued that the owner has implicitly consented to whatever copying or reproduction of the work is necessary to permit the Web page to be accessed and transmitted to the user. There can of course be no implied license when the copyright work has been posted or placed on a Web page without the permission of the copyright owner.

Similarly, where a copyright owner places a work on the Internet in such a way that it is freely available, it likely can be implied that any reproduction of the work necessary to permit the work to be perceived by a recipient (such as the loading of the work into the RAM of the recipient's computer) has been implicitly consented to. The availability of the work on the Internet does not, however, give an implied license to keep a permanent copy, pass a copy of the work along to another or alter or translate the work in any way. In effect, the Canadian law of implied license already provides for a type of "browsing exemption".[264] Again, if the work was not originally made available under the authority of

---

260 See Webster, "Copyright Exemptions", in "Important New Amendments to Copyright" (The Canadian Institute, June 27, 1996), at pp. 9-22.

261 *Hughes on Copyright and Industrial Design* (1984), at p. 450.

262 *Netupsky v. Dominion Bridge Co. Ltd.*, [1972] S.C.R. 368 at pp. 375-379.

263 Skone James, *Copinger and Skone James on Copyright*, (13th ed. 1991), at pp. 224-230.

264 Recommendation 6.4(a) of the IHAC Report stated that "it should be left to the copyright owner to determine whether and when browsing should be permitted". To the extent that this means that copyright owners should be able to decide whether to place copies of their works on the Internet, such a right is unobjectionable and already exists. It is unclear, however, how a copyright owner could purport to place a work on the Internet but not allow anyone else the right to view it. The placing of the work on the Internet where it is available to the public would seem to be the granting of implied license to browse the work, and such implied license would be inconsistent with the retention of any remaining control over the right to browse.

the copyright owner, there can be no implied license.

It must be noted, however, that there must be consent of the owners of all of the rights which could be infringed before there is implied consent, and it may be difficult or impossible for an Internet user to determine whether there has in fact been appropriate consent given. The downloading of what appears to be a single work may involve numerous copyright owners and different types of underlying rights. Even sophisticated copyright owners and users can be confused about the extent of the various rights which have to be licensed in order to make a work available on the Internet. Just because a work has been made available on the Internet by what appears to be a reputable rights holder does not mean that all appropriate clearances have been obtained.[265] As a result, reliance on implied consent may not be a very strong defence to a claim for copyright infringement on the Internet.

(g) Conclusion

As can be seen from the above discussion, there is no easy answer to the question "Who infringes copyright on the Internet?". The answer is clearest at the margins of the problem: Internet pirates, hackers and everyday users who deliberately reproduce, communicate, modify and distribute unauthorized copies of copyright works in Canada are liable for a copyright infringement. Even if the communication between such infringers are "private", a new infringing reproduction is made by the poster and the recipient each time the work is passed from person to person.

The issue becomes more complicated when the infringement does not occur wholly in Canada. Even if the poster is outside of Canada, there would still appear to be a copyright infringement if the Internet message containing the infringing material was available in Canada. It is possible that some intention on the part of the poster to send the message to Canadian users is necessary.

Internet intermediaries can also be liable for copyright infringement, but only in limited circumstances. If the intermediary is a direct participant in the infringement, it will be liable as a joint infringer. For example, direct participation could involve setting up a BBS or other site specifically for the posting of infringing copyright material.

Internet intermediaries which perform a conduit or carrier function are not liable for the infringing actions of their users, even if it is the intermediary's equipment and systems which are being used to infringe. In certain circumstances, Internet intermediaries could be liable for either authorizing infringement by users or, if they have the requisite knowledge, for indirect infringement pursuant to Section 27(4) of the *Copyright Act*. It is

---

265 See Segal, "Dissemination of Digitized Music on the Internet: A Challenge to the Copyright Act", 12 Santa Clara Comp. & High Tech. L.J. 97 (1995), at pp. 113-120 for a discussion of the same issue under United States copyright law.

difficult to assess the risk of such liability in advance, since liability will depend on the specific acts and knowledge of the Internet intermediary in respect of the particular infringement alleged.

5. LOOKING TO THE FUTURE

Although many say the Internet should remain an unregulated "Wild West", it is relatively certain that governments worldwide will increase their efforts, both individually and in concert, to attempt to impose controls on both the structure and users of the Internet.[266]

In Canada, the most recent phase of the ongoing revision of the *Copyright Act* has not dealt specifically with Internet issues. The recommendations of IHAC for amendments to the *Copyright Act*[267] have not been implemented and no timetable has been set for the "Phase III" amendments which might deal with such issues as database protection and the Internet. The time and effort which has been spent on Bill C-32 (which likely will not be passed until sometime in 1997) makes it unlikely that the Phase III amendments to the *Copyright Act* will be introduced any time soon.

Because the bases for the liability described in this study are necessarily speculative, and it is unlikely that there will be many Canadian judicial decisions which will clarify these rights in the near future, Internet participants must consider what steps can be taken to limit or control their potential liability. The preventative actions which Internet participants can engage in fall into roughly six categories: contractual limitations, warnings to users who might infringe insurance against liability, avoidance of high risk activity, technological controls and vigilante action.[268]

The least clear areas of liability on the Internet involve intermediaries which must deal with many users, mostly anonymous or nearly so, and many thousands of transactions each day. It is critical that Internet intermediaries have their relationships both with users and other Internet intermediaries well defined contractually in respect of potential copyright infringements. In particular, Internet intermediaries must obtain contractual undertakings from users with whom they have direct contact that the users will not infringe copyright. Such agreements may be of some use if the intermediary is forced to seek indemnity from the user on a copyright infringement claim by a third party, but, more importantly, such agreements will be an indication that the intermediary was not participating in or condoning the user's infringing activities. An alternative to a contractual relationship might be on-line warnings to users not to infringe copyrights. Similarly, Internet intermediaries should try to ensure that their contracts with the other members of the Internet transmission chain deal with potential liability for copyright infringements.

---

266 Knoll, "Any Which Way But Loose: Nations Regulate the Internet", 4 Tulane J. of Int. and Comp. Law 275 (1996); Hayes, "Canada, Cultural Sovereignty and the Internet", 1-4 *Cyberspace Lawyer* 13 (1996)

267 See, in particular, recommendations 6.3, 6.4, 6.5, 6.6 and 6.16 contained in the IHAC Report.

268 See Perritt, "Law and the Information Superhighway" (1996), at pp. 458-464 for a list of sixteen "alternative protection methods" which can be employed by owners of copyright content to protect their works from "free riders". Most of these methods fit into the six categories discussed below.

This study did not receive any submissions from insurers concerning Internet copyright infringement insurance, but it is understood that such insurance is in fact available. Broadcasters normally have insurance which covers claims for defamation and unintentional copyright infringement. While it is likely that similar products either are or will be available in respect of the Internet, insurers will likely set premiums too high until the nature of the risk is better defined and a loss history established.

One of the obvious ways for Internet participants to avoid liability for copyright infringement is to avoid activities which have a high risk that copyright will be infringed. Owners and hosts of Web sites must take care to ensure that they own or have licensed all rights to any copyright material included on the Web site. BBS operators must ensure that they do not encourage infringing activities by, for example, setting up forums to exchange copyright software or other works. The ethos of the Internet is changing, and those who continue to operate without regard to the rights of copyright owners will eventually pay a heavy price.

Technological controls which permit on-line protection of copyright works are only beginning to be developed, but likely are the future of copyright protection on the Internet.[269] Both Article 11 of the WIPO Copyright Treaty and Article 18 of the WIPO Performances and Phonograms Treaty require member states to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures"[270] used by rights holders to protect their rights.[271] It is not necessary that such controls be wholly "hacker-proof". So long as the vast majority of the population has neither the ability nor the inclination to bypass the control mechanisms, the system will work effectively to protect the interests of copyright owners.[272]

---

269 See Kim, "Taming the Electronic Frontier: Software Copyright Protection in the Wake of *United States v. LaMacchia*", 80 Minn. L. Rev. 1255 (1996) (arguing that criminal copyright infringement sanctions are unlikely to be effective on the Internet and that a combination of electronic copy protection and strategic civil actions against infringers must be employed to control piracy).

In a submission to this study, the Canadian Recording Industry Association (CRIA) indicated that the International Standard Recording Code (ISRC) provides a means for identifying digital copies of sound and video recordings worldwide. The ISRC has been adopted by the International Organization for Standardization as ISO 3901. It is still too early to tell whether this or some other standard will be generally accepted internationally as the appropriate methodology for marking digital copies.

270 The wording of the provision is somewhat curious, since a technological measure used by rights holders to protect their rights can hardly be said to be "effective" if it can be circumvented by some technological means.

271 See also Article 12 of the WIPO Copyright Treaty and Article 19 of the WIPO Performances and Phonograms Treaty concerning rights management information.

272 "The success of a copyright scheme does not lie in its comprehensive effectiveness so much as in its successful maintenance of an environment within which the vigorous production of goods continues to be worthwhile": Zimmerman, "Copyright in Cyberspace: Don't Throw Out the Public Interest with the Bath Water", *1994 Annual Survey of American Law* 403 at p. 412; "The goal for the future should be to stop amateurs from infringing and to make the costs of infringing for hackers and other professionals outweigh the benefits. Copyright infringement will be greatly reduced when compliance with the laws

Vigilante action against copyright infringement is intended to embarrass infringing users into stopping their infringement. One software company, Custom Innovative Solutions (CIS)[273] has made some of its computer software available on the Internet on an honour system which expects users to comply with the specific terms of the license set out on its Web page. The users which comply are added to CIS's "Winners" page, while those companies and individuals which do not are vilified in a "Losers" page.[274] The idea of this and other vigilante strategies is to make the cost of paying for the software lower for a company or individual than the cost of the embarrassment caused by the "Losers" appellation.[275]

It will always be important for creators and owners of copyright in works to take action against infringers, especially those who infringe in a systematic, large-scale manner which impacts on the commercial exploitation of a work by its rightful owner. It must be noted, however, that it has not generally been the practice in Canada for copyright owners to take widespread action against individual minor infringers since it is perceived that such action may backfire and alienate both potential customers and the government, the support of both of which is necessary to ensure that appropriate copyright protections continue to be available in the future.[276]

---

is the easiest choice for the user": Meyer, "National and International Copyright Liability for Electronic System Operators", available at http://law.indiana.edu/glsj/vol2/no2/meyer.html.

273 Located at http://www.cisc.com.

274 See Loundy, "E-law: Are You a Copyright Loser?", 1-6 *Cyberspace Lawyer* 20.

275 In its ongoing dispute with newspaper and magazine publishers, the Periodical Writers Association of Canada has set up a "Hall of Shame" on its Web site to try to embarrass publishers who are insisting that freelance writers agree to sign over all electronic exploitation rights to their work without additional compensation: see http://www.cycor.ca/PWAC/offend.htm.

276 Fedewa, "Challenges and Implications of the On-Line Age for the Music Business", *1996-97 Entertainment, Publishing and the Arts Handbook* 337, at p. 341.

6. CONCLUSION

The Internet, or some variation of it, appears here to stay. The amount of content, some of it protected by copyright, which will flow through worldwide computer networks will continue to increase exponentially over the next few years. In addition, those networks will increasingly converge with traditional broadcasting and communications channels to produce the "information superhighway".

Copyright also appears here to stay.[277] The recently concluded WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty establish important new norms with respect to copyright and neighbouring rights in the digital environment. In particular, the inclusion of provisions relating to on-demand communication over computer networks and technological protection measures for rights holders point the way towards a more comprehensive and national copyright regime in cyberspace. The continued application of copyright law to the Internet will be a major determinant of the future success of both the Internet and copyright law itself.

As this study demonstrates, copyright law principles can be applied to the Internet, although there is still uncertainty and much depends on individual facts in a particular situation. The Internet need not be lawless, at least in respect of copyright.

What is required now is a dialogue between copyright owners and responsible Internet participants to clarify areas of uncertainty and assist in determining future revisions to both the *Copyright Act* and international copyright conventions in order to deal specifically with the Internet and other computer networks. The failure to engage in this dialogue will leave the field open for the courts to define copyright liability on the Internet on a case by case basis, which may or may not produce sensible policy. The Internet and its potential for global communication seems too important to leave solely to judges and individual litigants who may not have any interest or understanding of the wide-ranging policy issues surrounding the Internet.

[Cat. N.: C2-312/1997E ISBN: 0-662-25489-9]

---

277 The early calls for the Internet to be a "copyright-free zone" have almost disappeared. Copyright will be adapted to deal with the Internet and its successors, just as it has adapted to previous technological changes. "Since the birth of copyright, every age has been the emergence of a new medium of expression or technology that has led people to express the fear or concern that it defined the boundaries of existing doctrines or that a new candidate for protection was so strikingly different that it required separate legal treatment. These apprehensions were voiced about photography, motion pictures, sound recordings, radio, television, photocopying and various modes of telecommunication. In each instance, the copyright system has managed over time to incorporate the new medium of expression into the existing framework.": Miller, "Copyright Protection for Computer Programs, Databases and Computer-Generated Works", 106 Harv. L. Rev. 977 (1993), at p. 982.

CONCLUSION: THE CHALLENGES AHEAD

0.1 The challenges of ... applying existing laws.

The newness of the Internet revolution and the fact that the Internet is put to new uses and employs new methods of communication on a daily, if not hourly, basis by millions of participants make it difficult to apply existing laws. However, the results of our study reveal that thus far, and in most situations, no glaring problems have been found which would mandate a massive legislative intervention.

We suggest that prudence commands that the legal policy analysis should first determine if existing laws can be interpreted to cover the new situations created by the Internet. The new situations should be analysed by first going back, if necessary by analogy, to the basic underlying principles of the individual statutes or laws being considered. In our opinion, new factual situations do not necessarily require either new legal theories or new legal solutions.

In some instances it may be useful for those who will have to analyse the impact of these new situations to proceed by way of analogy. By way of example, the various participants in the creation and distribution chain of content circulating on the Internet can be compared by resorting to the following metaphors:

- publisher: for those who create and/or publish content over which they exercise control;
- bookstore: for those who distribute material without control over its content but who may acquire a liability once apprised of the illegal nature of such material;
- broadcaster: for those who exercise control over some content, but not over other content, e.g., Usenet groups being compared to statements made by members of the public on live TV shows or, in some cases, where knowledge of content exists or is imputed, on taped TV shows;
- telecommunication common carriers: for those who only provide access to the Internet;
- landlords or hotel owners: for acts done by their users or subscribers without their knowledge or consent, etc.

Having said this, the authors are acutely aware of the limitations of saying that the Internet "is just like" something else. All such analogies are by their very nature limited and incomplete. While an analysis can begin with an analogy, it is both bad policy and bad law to fail to go further and note the areas in which the metaphor fails, is incomplete or is misleading.

In the situations examined under the Canadian legal system, we have found that the most difficult cases are not those of direct infringement (whether of privacy, intellectual property, Criminal Code, etc.) but those of indirect infringement where different standards apply to determine if the indirect infringer is liable depending on the statute involved (e.g. the

participation provisions of the Criminal Code, the right of authorization under the *Copyright Act* or the vicarious liability under civil and common law) or on the jurisdiction involved..

In general (and generalizations should be avoided for the reasons we have expressed above), we have observed that, except in those cases where direct infringement is involved, the more knowledge one has of the content and of its illegal nature (before the fact or even after the fact where content remains under the person's control) and the more control (not necessarily technical but certainly editorial) a person has over that content, the more likely that person will be held liable.

Viewed narrowly, these observations might bring some participants in the Internet content distribution chain to come to the conclusion that "the less you know, the better you are". Such a conclusion would, in our opinion, be socially, if not legally, irresponsible. However, our focus groups have revealed that such attitudes are not prevalent, at least among the major participants in the Internet distribution chain. It is hoped that through voluntary codes of conduct such as the one adopted by the Canadian Association of Internet Service Providers (CAIP) - see Appendix III - or the model code for the protection of personal information adopted by the Canadian Standards Association (CSA) - see Appendix IV, any remnant of these attitudes can be overcome. In time we believe that interested parties will come to the conclusion which most major participants have already reached: that it makes good (business) sense to be good citizens.

In this regard, we invite all those involved (and, in particular, publishers and disseminators of content) to adopt business practices to minimize their legal exposure by:

- implementing contracts and acceptable use policies with their subscribers and users that would clearly indicate what uses are permitted on their sites and to exclude their liability where the acceptable use policies have not been followed;
- reviewing any questionable material within their knowledge or control or material brought to their attention after the fact;
- establishing a policy for dealing with potentially illegal situations discovered by them or brought to their attention by other users, enforcement officials or private complainants; and
- obtaining legal opinions where prudence would dictate so, in addition to educating themselves on the limits between the permissible activities and the potentially illegal activities.

Moreover, because employers may also be held liable for acts of their employees, we invite employers to adopt similar measures which could be added to the existing "software use policies" that many of them already have, prohibiting, among other things, unauthorized reproduction of software.

In addition, we hope that through the evolution of the case law, legal standards will evolve such that the threshold required to be found not liable will involve consideration of the adoption of reasonable measures by Internet participants such that "wilful blindness" will in itself be a factor considered in determining liability.

In the researchers' opinion, laws should be modified only when it becomes clear that changes are necessary.

Where it can be reasonably interpreted that current laws will be applicable, we suggest that the prudent policy approach should be to wait and see how the courts apply existing laws to the Internet paradigm. Only if it becomes necessary as a result of unexpected judicial interpretations of existing laws should the laws be amended to adjust to the new situations and then, only as strictly necessary.

However, in those cases where it is clear that certain statutes should be amended or if the risk for society is too high that certain statutes be held inapplicable or be held applicable, as the case may be, to a given situation the legislator should intervene.

In all cases where certain statutes need to be amended, the legislator should intervene to amend the statutes in a *de minimis* way and in a way as technologically neutral as possible under the circumstances.

We also suggest that these amendments should aim at balancing the interests of the users, publishers and disseminators of content on the one hand, and those of the authors, on the other, while preserving freedom of expression and only imposing limits on such freedom where necessary in a free and democratic society. In this regard, the scope of the study excluded any consideration of the possibility that certain activities on the Internet be subject to regulation by the Government.

Those who encounter situations where they think existing laws are inadequate and should be modified, should not hesitate to report these situations to the Government for review and, potentially, legislative correction.

0.2 The challenges of ...enforcement

The volatile nature of the many activities conducted on the Internet, coupled with the possibility for participants to remain anonymous and the international aspect of most Internet "transactions", make it very difficult to detect illegal activities and to enforce existing laws.

On the other hand, however difficult the new technical revolution may render such detection and enforcement at an early stage, it also offers new possibilities to detect illegal activities and to enforce existing laws.

In our opinion, these enforcement difficulties in themselves do not create a need for the amendment of existing national laws. Rather, these difficulties mandate the establishment of new methods of international cooperation for detection and enforcement, be it by way of formal international treaties or informal international working arrangements between private interest groups or national police forces.

0.3 The challenges of ... abiding by existing laws

Even assuming, as we do, and as our focus groups have revealed, that the great majority of users, creators and disseminators of content are law abiding citizens, the current state of technology has created many opportunities for millions of people to break the law, often unknowingly.

In situations where a guilty intent ("*mens rea*") is not at issue (such as in the case of civil actions for direct copyright infringement), innocent persons may be held liable for infringement.

On the Internet, for a given factual situation, different standards may apply, such as different burden of proof standards between civil and criminal law, different community standards between different parts of the country for certain obscenity-related situations, different legal standards between civil and common law. Such differences increase exponentially in the Internet world because the same situation could cause the laws of many different countries to apply. A prudent approach therefore mandates that users, publishers and disseminators of content apply to their conduct the highest common denominator mandated by the application of all major legal systems. By way of example, international site operators who collect information about their subscribers and users "consumption habits", whether directly or through the use of "cookies" (those few lines of codes that reside on a user's computer, most often without the knowledge of the user, to enable the site to recognize the user in future accesses to the site) should abide by the European Union legislation respecting the collection and use of personal information and the Québec Act respecting the protection of personal information in the private sector, which are presently, to our knowledge, the most demanding laws requiring protection of personal information.

The focus groups have permitted us to appreciate that, in Canada, some of those involved in the dissemination of content make substantial efforts to ensure compliance with the existing laws as they understand them. These efforts are to be commended, should continue, and should be encouraged to extend to all stakeholders.

In addition, those who have interests to defend should actively participate in public education campaigns to educate all involved to abide by existing laws.

As well, all the stakeholders should be encouraged to get together, as software users get together with software publishers, to discuss needed improvements in computer programs, to formulate codes of conduct, policies and other common solutions acceptable to all.

0.4 The challenges of ... Internet paradises

Where the legal systems of some countries do not appear to provide adequate solutions to deal with the situation, and in order to avoid the formation of "Internet paradises" in these countries, strong international cooperation is required to bring protection in these countries more in line with those of countries who provide higher levels of protection.

It should also be remembered that, in this regard, the legislator should balance the interests of all involved including users, creators and disseminators of content. The introduction of legislative changes, or the failure to introduce legislative changes deemed by these groups to be required, can cause these groups to establish their activities in countries which they perceive as being more advantageous to their interests. Consequently, Canada should seek to maintain a balance between the rights of all stakeholders while preserving the basic values of freedom of speech, privacy and prohibition of offensive material cherished by the Canadian society.

The Internet does present challenges not only from a legal perspective, but also from social, technological, economic, political and cultural view points. It also offers tremendous opportunities for the advancement of social, economic and political objectives and, in particular, for the development of less developed countries.

The researchers hope that the benefits will far outweigh the disadvantages and that this study provides a useful contribution to the identification and resolution of liability issues arising in the Internet content dissemination chain.

[Cat. N.: C2-312/1997E ISBN: 0-662-25489-9]

APPENDIX I

CONTENT-RELATED INTERNET LIABILITY STUDY

TERMS OF REFERENCE

PURPOSE:
To produce a well researched and balanced document on content-related Internet liability for Internet service providers (ISPs), Bulletin Board Services (BBSs), newsgroups and other related services. The document will also discuss information controls, privacy issues and the protection of works and describe policy models presently discussed or implemented in Canada and other OECD countries.

STUDY GUIDELINES:
This study of content-related Internet liability will assume that liability is possible on the Internet. The issues to be clarified include, *inter alia*, who is or should be liable, but not the separate issue of whether Internet services should be regulated under telecommunication or broadcasting legislation. Finally, this study's priority task is to describe the environment and issues related to provider liability -- its purpose is not to elaborate policy options or formulate recommendations.

This study will help all participants in the content value chain better understand their roles regarding information management liability and the effect of their activities and decisions on other stakeholders. It will provide the key information needed in managing the rights and obligations of the Internet in Canada.

BACKGROUND:
Internet service provider liability is increasingly important for all participants in the Internet content value chain, whether they are creators, producers/publishers, equipment manufacturers, distributors, information brokers, carriers, business users, consumers or access providers. Unfortunately, the role of ISPs and other related services in this chain is confusing. Many characterise their present and anticipated services on a continuum between carriage and content. Their activities range from transporting bytes, distributing content previously selected by their service provider, distributing content of previously selected publishers and distributed, linking to other content providers and providing facilities to third parties to make available and exchange various types of documents. Confusion also exists as to how service providers may monitor and control the behaviour of users, while ensuring their privacy. The fact that ISPs and other online services provide access points to the Internet suggests to legislators, interest groups and copyright holders that providers may have possibilities of control.

Previously, the Internet was small enough to be self-governed, mostly by those in academic and research circles. It has, however, experienced rapid, explosive and global growth in content, use, applications and access points. New information content services have evolved, including access to sophisticated databanks, computer bulletin boards and electronic mail services. Through these services, text, graphic, audiovisual and audio documents are made available and exchanged.

Participants in the information content value chain must now address the new challenges digitized works carried over global networks create, such as the ease of reproduction, adaptation and communication of these works. These challenges combined with the Internet's explosive growth create new issues in governance and render the old model of sole reliance on self-regulation as unworkable.

The newness of the ISP industry aggravates the lack of clarity regarding these issues. No significant data on revenues and profits, market share or ownership profiles, nor on the nature of services available in the market exists. The convergence of technologies, industry activities and markets further exacerbates attempts to apply existing laws to the new environment, and underscores their complexity (i.e., by increasing the potential of overlap between traditionally separate laws).

ISP liability has only recently received serious scrutiny. The US National Information Infrastructure Task Force examined this issue in light of copyright considerations and tabled its findings in 1994. The Canadian Information Highway Advisory Council (IHAC) tabled a series of recommendations in September 1995, notably in the areas of information controls (e.g., hate literature and pornography), privacy and copyright. IHAC recommended harmonising information control legislation and that the federal government "take immediate steps to lead in the development of legislative measures with regard to clarifying the question of liability of owners, operators and users of bulletin boards, Internet and Usenet sites."

IHAC's Subcommittee on Copyright addressed the issue of "copyright liability with respect to carriage of protected works," but considered the issue more for electronic BBS operators than for common carriers. IHAC'S recommendation 6.16 confirmed BBS operator liability, but requested that in the absence of a defence mechanism, no "owner or operator of bulletin board systems should be liable for copyright infringement if a) they did not have actual or constructive knowledge that the material infringed copyright; and b) they acted reasonably to limit potential abuses."

More recently, the SOCAN, a collective responsible for collecting royalties for authors and composers of musical works and their publishers, tabled a tariff with the Copyright Board to be paid by ISPs for the public performance of musical works available on the Internet.

Obscene material, child pornography, and hate propaganda have been made available on the Internet in various means -- on World Wide Web (WWW) and ftp sites, Usenet newsgroups and private computer bulletin board systems. Yet the issue of the liability of service providers and users requires clarification because of the variety of services, ownership and degrees of cognizance. On what grounds, for example, can one determine a difference in liability between an ISP that owns and operates a WWW site with illegal material and an ISP that permits its subscribers to create and maintain their own WWW sites, one of which may contain illegal materials? Similar problems arise with respect to ftp sites and BBSs that provide file archives and the facility for user uploads. The question of Usenet newsgroups is particularly difficult -- at what

point is there liability in providing access through one's server to a group's files, where some files may sometimes contain unforeseeably illegal messages?

Although domestic legislation and interpretations are needed, the Internet is not contained within a single jurisdiction or country. The international or global nature of Internet services means that any domestic legislation has to consider an international context and the thorny issue of how to deal with countries with divergent legislation or with no legislative framework.

To avoid unsought and unnecessary litigation, ISPs may need to adopt clear acceptable use or editorial policies. These would address such issues as: recognition of any outstanding liability; danger of perceived arbitrary decisions; making decisions in light of divergent community values; reconciling approaches with the firm's good corporate citizen policies; and the tradeoff of introducing built-in monitoring capabilities into the architecture of services.

CASE LAW:

Case law, legislation and policy documents developed in OECD countries provide some guidance as to the nature and scope of liability to which Internet Service Providers may be subjected. In the United States, for example, there have been cases in the last three years involving Internet Service Providers that have examined the issues of copyright infringement, obscene materials and defamation.

In the copyright infringement area, US courts have examined the issue of ISP liability in cases including *Playboy* v. *Frena, Sega Enterprises Ltd.* v. *Maphia,* and the three recent cases involving the Church of Scientology, *(Religious Technology Center* v. *NetCom On-Line Communication Services Inc., et. al., Religious Technology Center* v. *Lerma, et.al*., and *Religious Technology Center* v. *F.A.C.T. Net, Inc.)*. In addition, the issue of the financial liability of ISPs for the transmission of copyright material to end users who could browse, listen to and download songs was initiated in the *Frank Music* v. *CompuServe Inc.* case, although that case ultimately settled before going to trial. The issue of liability with respect to obscene material was examined in a 1996 case before the U.S. Federal Court involving violation of federal obscenity laws, *U.S.* v. *Thomas*. Finally, the issue of defamation was before the court in the case of *Cubby* v. *CompuServe Inc*. The cases may also raise the issue of what position the ISP occupies in the Internet content value chain, by addressing the issue of whether the ISP is found liable under direct, contributory or vicarious liability.

The U.S. Congress also recently addressed the issue of Internet Service Provider liability in the Communications Decency Act of 1996 (Title V of the *Telecommunications Act of 1996*). Activists took court action in favour of on-line freedom of speech, press and association, initially seeking a preliminary injunction with respect to the provision dealing with criminal penalties for "indecent" but constitutionally protected telecommunications to individuals under the age of 18 and one which criminalizes the use of any "interactive computer service" to "send" and "display in a manner available" to a person under 18 any communication that "depicts or describes," in terms patently offensive as measured by contemporary community standards, sexual or excretory

activities or organs." A preliminary injunction was granted and, in a subsequent decision of the U.S. Federal Court (June 12, 1996), the Court ruled these provisions unconstitutional. The government is expected to appeal this decision to the U.S. Supreme Court.

The September 1995 report of the Working Group on Intellectual Property Rights, "Intellectual Property and the National Information Infrastructure (NII)," examined the ISP liability issue and concluded that it is at best premature to reduce the liability of any type of service provider in the NII environment.

In Canada, in the spring of 1995, eleven BBS operators were raided in the greater Montreal area. Persons were charged under the Copyright Act based on their activity of making available copies of pirated Canadian software. In May 1996, the first defendant appeared in court, having applied to the court in February to have some of the evidence excluded on constitutional grounds. The court denied the application. The court said, among other things, that there should not be any "reasonable expectation of privacy" with respect to persons who use BBS for communications purposes, when the BBS is run as a private enterprise. Thus, the court said, police can put a BBS under "electronic surveillance" and keep a verbatim electronic record of communications with the computer and with individuals in these circumstances. In British Columbia, BBS operators were charged in the fall of 1995 under the obscenity and child pornography sections of the Criminal Code.

OBJECTIVES OF THE STUDY

1. Describe ISP and related services (BBS, newsgroups and on-line services) in relation to the content value chain;
2. Examine appropriate case law in Canada and the US and the possible impacts on all major stakeholders with respect to provider roles and responsibilities, liability criteria and trends or divergencies in court decisions;
3. Discuss the various issues involved with liability, in the areas of copyright as well as information controls and privacy; these issues include liability management issues; and
4. Describe the key policy models, including self-regulatory discussed or implemented in OECD countries.

The study will help all participants in the content value chain better understand their roles with respect to information management liability and the impacts of their activities and decisions on the other stakeholders; it will provide key information to assist them in managing their rights and obligations in Canada. Major stakeholder organizations will be invited to be part of focus groups in Vancouver, Toronto and Montreal to share their views and concerns, as well as submit views and concerns in writing.

Documents will be written in plain language and reflect in a balanced manner the positions of the stakeholders. They will focus on industry issues as perceived by industry, be based on extensive research and provide an executive summary that will be a useful tool for industry and government

executives. No legal conclusions or opinions are requested under this contract. All documents are to be submitted in WordPerfect.

MILESTONES:

1. Detailed outline and list of planned focus groups and contacts representing the major stakeholders **(August 1, 1996)**
2. First draft of main chapters **(October 1, 1996)**
3. Penultimate draft of full report **(October 21, 1996**
4. Final report with executive summary **(November 12, 1996)**
5. Upon request, a maximum of four presentations to Industry Canada and industry associations (travel costs covered)

[Cat. N.: C2-312/1997E ISBN: 0-662-25489-9]

APPENDIX II: List of Submissions

Alliance of Canadian Cinema, Television and Radio Artists

Association for Media and Technology in Education in Canada

Book and Periodical Council

Burnett, Daniel W.

Canadian Association of Internet Service Providers (CAIP)

Canadian Association of Law Libraries

Canadian Conference of the Arts/Conférence Canadienne des Arts (CCA)

Canadian Copyright Institute

Canadian Recording Media Association

Canadian School Boards Association

Educational Media Producers and Distributors Association of Canada/Association des médias et de la technologie en éducation au Canada

Independent Film & Video Alliance

National Library of Canada/Bibliothèque nationale du Canada

Office for Disability Issues - Human Resources Development Canada/Développement des ressources humaines Canada

Patent and Trademark Institute of Canada/Institut des brevets et marques de commerce du Canada

Periodical Writers Association of Canada

Special Libraries Association - Government Relations Committee

Stentor Telecom Policy Inc.

Sutherland, Dave

Time Warner Inc.

Torstar Corporation

APPENDIX III

The Canadian Association of Internet Providers (CAIP)
"CODE OF CONDUCT"

NOTE: RE: COMMENTARY: The commentary provided after each principle is merely to assist with the interpretation of each of the seven priciples and procedures set out in the CAIP Code of Conduct. This code is voluntary for CAIP members.

1. CAIP will cooperate with all Government officials, international organizations and law enforcement authorities seeking to clarify the responsibilities for each of the different functions performed by Internet companies.

***Commentary*:**

1.1 Although there are no Internet-specific laws at present, it is conceivable that each different service provided by Internet access and technology suppliers may attract a differing policy or legal regime. For instance, point to point communication such as email and file transfers might be treated differently by legislators and courts than services for the creation or hosting of Web sites, or for the storage and retransmission of content such as newsgroups, and on-line video or audio services.

2. CAIP members pledge to comply with all applicable laws.

Commentary:

2.1 The primary purpose of this Code is to assist CAIP members with the development and implementation of internal policies and practices to comply with existing legal standards.

2.2 Each CAIP organization may tailor its own methods to meet its particular circumstances.

3. CAIP members are committed to public education about Internet issues and technology.

Commentary:

3.1 Many current proposals for assigning liability for content and Network abuse do not correlate to the actual design and function of various Internet services. CAIP believes that a better understanding of the technology will help all Canadians understand the options available to all stakeholders (including the broad range of users, technology suppliers and policy makers).

4. Privacy is of fundamental importance to CAIP members who will respect and protect the privacy of their users. Private information will be disclosed to law enforcement authorities only as required by law.

Commentary:

4.1 CAIP members should establish internal procedures to protect personal privacy regardless of the form in which such information is stored, and taking into account the relative sensitivity of each type of information.

5. CAIP members will not knowingly host illegal content. CAIP members will share information about illegal content for this purpose.

Commentary:

5.1 The Internet is designed to route around blockages, therefore, despite any effort or step taken by a CAIP member, users who wish to obtain or publish illegal content may be able to obtain it from sources or sites outside the control of CAIP members.

5.2 Sharing information about material that has been evaluated as illegal will facilitate some preventative action.

6. Although Internet providers are unable to monitor all content, CAIP members will make a reasonable effort to investigate legitimate complaints about alleged illegal content or network abuse, and will take appropriate action.

Commentary:

6.1 Due to the impracticality of surveying content on the World Wide Web and Usenet sites, CAIP has elected to deal with content and abuse issues on the basis of a complaint-driven process.

6.2 Information about the procedures to receive and respond to complaints or inquiries established by each CAIP member, shall be made available to users. However, what constitutes appropriate action will vary depending upon the results of the investigation in 7.0 (below), and on what role the CAIP member has played in the transaction or activity at issue.

7. Prior to taking any action, upon receipt of such complaints CAIP members will:

a) conduct an internal review to determine the nature and location of the content or abuse, and where warranted;

b) consult with legal counsel and/or outside authorities, and/or;

c) notify the content provider or abuser of the complaint, with a request for a response within seven days.

Commentary:

7.1 Notice is generally only given when the abuser is a customer of a CAIP member or the illegal content has been published by a customer of the CAIP member.

Please send your comments about the code to CODE@caip.ca

[Cat. N.: C2-312/1997E ISBN: 0-662-25489-9]

APPENDIX IV

First Edition of CSA Standard CAN/CSA-Q830
MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION (Summary)

Principles in Summary
Ten interrelated principles form the basis of the CSA Model Code for the Protection of Personal Information. Each principle must be read in conjunction with the accompanying commentary.

1. **Accountability**: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. **Identifying Purposes**: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent**: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. **Limiting Collection**: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention**: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6. **Accuracy**: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness**: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access**: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance**: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

For more information, consult - http://www.csa.ca/83001-g.htm
[Cat. N.: C2-312/1997E ISBN: 0-662-25489-9]