Law of Cyberspace Series

Volume 1

The International Dimensions of Cyberspace Law

Ashgate
DARTMOUTH
Aldershot • Burlington USA • Singapore • Sydney

UNESCO
Publishing

Law of Cyberspace Series, no. 1
Bruno de Padirac, General Editor
This volume edited by Teresa Fuentes-Camacho

Published by
Ashgate Publishing Limited
Gower House
Croft Road
Aldershot
Hants GU11 3HR
England

Ashgate Publishing Company
131 Main Street
Burlington
Vermont 05401–5600
USA

Ashgate website: http://www.ashgate.com

Published jointly with the United Nations
Educational, Scientific and Cultural Organization
7, place de Fontenoy, 75352, Paris 07 SP, France

British Library Cataloguing in Publication Data
The International Dimensions of Cyberspace Law.
(Law of Cyberspace)
1. Information superhighway—Law and legislation.
I. Fuentes-Camacho, T.
341.7'577

Library of Congress Cataloging-in-Publication Data
The international dimensions of cyberspace law/edited by Teresa Fuentes-Camacho.
p. cm. (Law of Cyberspace series)
Includes index.
ISBN 0–7546–2141–3 — ISBN 0–7546–2146–4 (pbk.)
1. Data transmission systems—Law and legislation. 2. Computer networks—Law and legislation. I. Fuentes-Camacho, T. II. Series.
K564.C6I565 2000
341.7'577—dc21 00–34845

Ashgate ISBN 0 7546 2141 3 (Hbk)
ISBN 0 7546 2146 4 (Pbk)
UNESCO ISBN 92–3–103752–8

Typeset by Manton Typesetters, Louth, Lincolnshire, UK.
Printed in Great Britain by MPG Books Ltd, Bodmin, Cornwall.

5 Liability in Cyberspace[1]

PIERRE TRUDEL

INTRODUCTION

The advent of cyberspace, as a place of interaction, brings the question of the apportionment of responsibility among participants in electronic communication more acutely to the fore. In most countries, there is debate on who is answerable for the information circulating on open networks such as the Internet. Now that we have outgrown the idyllic conceptions of a cyberspace[2] which evades all regulation and is exempt from any conflict, and with interaction in these virtual places on the increase, the most pressing issue is that of liability. There is no escaping the question as to 'who' is answerable for information that has caused conflict or damage. It is in the laws of the different territories and countries that firm guidance on these questions is to be found.

In order to deal with this aspect, it is important to specify the scope of the problem of liability in cyberspace – a fairly new area for law. The heuristic approaches that are used to isolate the respective responsibilities of the different participants in electronic communication must then be tackled.

CYBERSPACE

Cyberspace[3] is an undefined area. It is the continually provisional consequence of the interconnections existing among computers connected in accordance with compatible protocols. Its morphology is determined by the software tools used and the links existing between the sites and the data. Thus the hypertext that is a feature of the World Wide Web produces a continually redefined and unpredictable space, fluctuating with the links that the users decide to

activate. The course followed by each of the participants in electronic communication depends on the choices he or she makes and the links available.

Cyberspace has four characteristics which assume importance when the problem of its regulation is considered. It is virtual space, a place for interaction, and it is characterized by the sovereignty of the user and by competing regulations.

Virtual Space

Cyberspace is not situated at a specific point in territorial space.[4] The possibility of controlling activities that take place in it has little to do with the physical location of the protagonists. It can be defined as virtual space resulting from the manifold interconnections made possible by the interoperability of the networks. Whereas, in the physical world, the location of persons and businesses within national frontiers is a basic premise of the applicability of the principles of the law of a particular state, in cyberspace everything is simultaneously present and absent at a given geographical position. A message is present wherever a computer is connected; all the states in which one of these points of reception is to be found can claim to apply their law. Few, however, are actually in a position to enforce it.

A Place for Interaction

The Internet is not just a place for broadcasting; it is much more a place for interaction. We must set aside the approaches based on the premise that this virtual space is used for broadcasting and concentrate on determining the scope of the problem of a regulatory framework for the activities going on in places of interaction. In respect of places of interaction, rules are less concerned with governing the dissemination of information than with providing a framework within which relations on the Internet may be contained. At least three areas of conflict almost always become apparent at some time or other in the environments of open or interactive networks.[5]

The first area of conflict concerns right of access to the networks: someone who is not in a network wants to gain access to it, whereas those who are already in it or who control it want to keep that person out. This type of conflict calls for a clarification of the principles governing the right of access to the networks. It presupposes the introduction of measures that will ensure equity or equality as regards access. Under what conditions should there be rules guaranteeing universal access? By what means can we ensure that

basic services are available to whole populations? How can what should be regarded as a basic service and what constitutes an optional service be differentiated? These questions concern the status of the networks, the principles of their operation and the rules governing rate fixing. Furthermore, the networks are coming increasingly under the control of private bodies. While they are gateways to cyberspace on a global scale, the networks are also gatekeepers that can, in practice, decide to exclude participants in electronic communication. The question of their responsibility thus arises in two respects: as gatekeepers and as holders of certain monitoring powers of an editorial nature.

A second area of conflict affects the flow of information. Some people want to prevent certain information from circulating, whereas others want to continue to broadcast or receive such information. Information that is defamatory or violates privacy can circulate in cyberspace. The circulation on open networks of material protected by copyright is another significant source of concern. Conflicts may stem from the desire of injured parties to obtain compensation for damage suffered as a result of the circulation on a network of harmful information. The legal system governing the determining of liability as a result of the circulation of information is therefore a major component of the infrastructure of electronic environments.

A third area of conflict involves the mechanisms designed to ensure that users of a network keep their word. The kind of conflict that arises when someone on the network believes that another person has not fulfilled his or her obligations calls for the establishment of an appropriate framework to facilitate the harmonious conduct of transactions. The question that then arises is whether bodies to stand surety for certain contractors exist.

The Sovereignty of the User

Because information highways give users greater control over their choices, they consequently, incur a larger share of liability for the interaction in which they agree to take part. The absence of any centralized control means that users have to bear the burden of ensuring their own protection: no one can relieve them of this burden and claim to offer guarantees against false or otherwise misleading information. On the Internet, individuals may be dealing with a business that adheres strictly to high standards, or they may be taking the risk of entering into a contract with an imposter.

The question of responsibility must therefore be examined against the background of this wider discretion which appears to be left to individual users. The challenge to each of the sites desirous of

holding its own is to offer optimum integrity, in accordance with the demands of consumers or users. Individual users can choose to visit only those sites that present guarantees of reliability and honesty or to take risks by visiting sites operating on the basis of rules offering few guarantees, if any. All in all, the option of evading regulations works both ways. In some cases, people will avoid a site because it seems too controlled and the rules in force do not suit them, whereas in other situations, particularly when integrity and credibility are required, they will be inclined to visit sites applying regulations that offer optimum guarantees of integrity and reliability. In these respects, the sites are in competition with one another, which entails competing regulations.

Competing Regulations

Electronic communication presupposes a voluntary act on the part of the user, to whom it gives the option of connecting up elsewhere. Moreover, anyone not satisfied with the rules applying in a network or a particular electronic environment can always set up other networks. This possibility has a major implication: regulation on the Internet is an activity open to competition; no authority can claim to exercise a monopoly over the laying down or the enforcement of rules.

Competition may concern the quality of the guarantees of integrity offered by each of the sites made available to users and the social pressure these users will bring to bear. If the rules do not suit the actors, they often have the option of changing their location so as to evade the unwanted rules. This means that when the problem of regulation in such an environment is tackled, the formal or state-inspired paradigms on which legal analyses are often based must be abandoned.

DETERMINING RESPONSIBILITY IN CYBERSPACE

In this section, the conditions under which the various participants in electronic communication may incur liability are set out. In order to cover the essential aspects of the question of responsibility adequately, we must refer to the principal metaphors illustrating what the persons involved in electronic communication are doing, and then draw up a list of the main factors which create liability for the circulation of information in cyberspace.

The Principal Metaphors

In cyberspace as elsewhere, the person who physically performs the tortious harmful act is, of course, the first to incur liability for it. However, in electronic environments that person is not always identifiable, or may be out of reach. Hence the importance of determining the responsibility of the other persons participating in the chain of the information transmission.

In many situations in which the circulation of information causes damage, the criteria for appreciating responsibility are based on the roles assumed by the different participants in the chain in adding value to the information. The incurring of liability rests largely on a comparison, or an acknowledgement, of similarities and differences existing in the systems developed for situations resembling communication in open electronic networks, such as, for instance, railway transport or the circulation of printed matter.[6] It is thus asked who acted as a publisher, a common carrier, a broadcaster, a newspaper and so on because the obligations and responsibilities attaching to these respective roles are well established in the law of liability. It is therefore by extrapolating from both the characteristics of the different communication contexts to be found on the Internet and analogies apparent in the roles and functions of the various persons involved that it is possible to sum up the situation as regards the law of liability resulting from the transmission of information on the Internet.[7]

In the law of a number of countries there is a close link between the control exercised over presumably harmful information and the ensuing liability. Thus the greater discretionary power to decide what will be published (or broadcast), the greater the liability incurred by such a decision.

In order to deal with the status and responsibilities of participants in electronic communication, it is a good idea to seek parallels in familiar communication contexts in order to find an adequate metaphor. Some writers advocate setting up a hybrid legal framework specific to electronic environments and taking over various concepts already applicable to existing channels of communication.[8] What helps give the impression of a so-called loophole in the law as regards the Internet is the absence of a consensus on the metaphors that should contribute to situating the roles of the participants in electronic communication, and also the various inadequacies inherent in each of these metaphors when it comes to illustrating the roles actually played in electronic communication.

While recourse to metaphorical analysis is likely to clarify matters for anyone seeking to define the responsibilities of the various persons involved, the limitations of such an approach are soon evident,

as has been demonstrated by a number of authors. Whereas, traditionally, communication contexts have been well compartmentalized,[9] the advent of electronic environments has created the impression that 'the legal system is trying to fit square pegs into round holes'.[10] Care should therefore be taken not to extend a type of regulation to electronic environments solely on the basis of their possible resemblance to pre-existing environments.[11]

When attempting to identify the components of this fundamental legal framework, it is timely to observe that a number of persons play a role in cyberspace. Each of these participants involves variations and recombinations, so that, in some situations, one and the same entity may assume more than one role. In environments such as the Internet, however, there are always network operators, information providers and one or more information carriers. According to the (often very fluctuating), circumstances, one or other of these entities may take on the role of a publisher, a librarian (or distributor), an owner of premises or a carrier of messages.

The Carrier

Some of the persons involved in cyberspace assume the role of mere carriers of information. The analogy with common carriers throws light on the conditions of liability of the administrator of an electronic mail server acting solely in that capacity.

In the same way as a carrier, an electronic communication system sometimes does no more than serve as a channel for transporting information from one site to another.[12] As a rule, common carriers are exempt from liability for the content of statements they are paid by their users to carry.[13] In contrast with publishers and distributors, carriers are under an obligation to carry any message without discrimination, be it with regard to the content of the message or the person who sends it.[14]

The Owner of Premises

Some writers have argued that electronic communication requires the use of a person's property.[15] This means that persons may find themselves in a situation in which presumably harmful information is found on premises which they own. So, what is the position in regard to the liability of owners under such circumstances?

Owners are seldom rendered liable for acts committed on their premises. For instance, when a hotel lets a room to a client, it has neither the obligation nor the right to supervise what that client does there and is therefore not liable for any illegal activities taking place there.

This argument is in keeping with a principle established in the judicial doctrine of a number of countries, according to which an owner is not necessarily liable for offences committed by tenants. Obviously, a hotel which knowingly makes itself a centre of illegal activities is liable for any damage, in the same way as the web site owner would be if he or she endorsed defamatory messages transmitted by users.[16] It is, after all, recognized that the owner of a property who, having been informed of the presence of libellous graffiti on its walls and who does nothing to have them removed is considered to be a repeater of the remarks and is liable for damages in the same way as their author.[17] Accordingly, a webmaster would always be under an obligation to withdraw information he or she knew to be harmful, failing which he or she would incur liability as a repeater of the remarks.[18] Thus, if the metaphor of the owner is applied to the webmaster, the prerequisite for liability would be knowledge of the presence of harmful information on a site.[19]

The Publisher

The publisher publishes information. Publishing means communicating information to third parties in the knowledge that the information will be read, seen or heard. As publication is effected intentionally, it presupposes knowledge of the content of the information transmitted.[20] In the context of the Internet, publication may result from the transmission of files, or of discussions in the context of electronic conferences, or again the making available of information in files that can be transferred via the network.[21] Thus an access provider to the Internet who examined all messages before retransmitting them and reserved the right to forward only those messages deemed in conformity with his or her policies would be behaving in the same way as a publisher.

In situations such as this, the decision to publish invariably rests with the publisher. For the publisher it is an option: he or she is under no obligation to publish. In the sphere of the press and publishing, it is usually held that the editor-in-chief, or the publisher, is in a position to control the information circulating as a result of his or her activity.[22] Liability for the transmission of harmful information is entailed by this power of control.

In *Stratton Oakmont Inc.* v. *Prodigy Services Co.*,[23] the New York Supreme Court found that the Prodigy network was assuming the role of a publisher. A Prodigy subscriber sent a defamatory message concerning the director of Stratton over the network through a bulletin board. The Court held Prodigy to be liable for the damages caused to the slandered person. In order to classify Prodigy as a publisher, the Court examined the behaviour of the webmaster with regard to

the information carried.[24] In this respect, Prodigy exercises some control over the information it carries, because its advertising announces a 'family' service. It must therefore eliminate any information that does not meet this criterion by employing, among other methods, software for censoring obscene material and personnel to examine messages and ensure that they are in line with Prodigy's policy. In this particular case, the Court found that the fact of using the technology required for the restriction of harmful messages was sufficient ground for concluding in favour of editorial control and triggering off liability: Prodigy incurred liability for the information it transmitted, since it was supposed to be acquainted with its content.[25]

Thus, in the case of a closed and controlled discussion list, it is reasonable to hold that the controller is analogous to a publisher and should therefore assume responsibility for what he or she forwards.

The Librarian

A librarian does not control the content of the information transmitted or made available to readers. For this reason librarians are not liable if that information proves to be harmful.[26] It would indeed be unthinkable for every distributor (newspaper vendor, bookshop, library) to be under an obligation to check the contents of every publication distributed to ensure that no offending, illegal or harmful information[27] was contained therein. However, distributors exercise certain choices of an editorial nature, often based on the guiding principles of their chosen calling.

On the other hand, it is recognized that librarians are under an obligation to withdraw information once they have been informed that it violates the law. If not, they may incur liability for the resulting damages.[28]

In *Cubby Inc.* v. *Compuserve Inc.*, an electronic message distributed in Compuserve contained disparaging remarks concerning a rival service provider (Cubby). The court found that Compuserve had no control over the information circulating in its system and that it could not, and had no reason to, know the harmful nature of the messages. There was therefore no liability. The court compared Compuserve with an electronic library. In the same way as a library, Compuserve had the option of circulating or not circulating a work, but once the work was in its system it had no editorial control over it. Furthermore, even if Compuserve had wanted to examine each message, their sheer numbers rendered this an impossible task.[29]

In addition, system operators often lack a legitimate reason for intervening and deleting potentially harmful information. In the name of what, and by virtue of what authority, have they to gauge the offensive or inoffensive nature of a piece of information? By virtue of

what authority should they set themselves up as judges with responsibility for determining whether or not a content is offensive and harmful?

The Principal Factors in the Incurring of Liability

A number of factors are taken into consideration when it comes to determining the existence and extent of liability incurred by one or another of the participants in electronic communication. Without claiming to be exhaustive, I note that, in a number of legal systems, the factors to which importance is attached are knowledge of the information and control – whether editorial or physical – over it. Also taken into account, in the case of certain types of information, are the expertise of the person who produces it, the foreseeability of the uses to be made of it, the role of the user, the context, and the accessibility of the information.

Control over the Information

In order to determine the liability of someone who transmits the same information to several users at the same time, it is necessary to consider that person's relationship to the content of the message transmitted.[30] This criterion of control appears even to be a prerequisite for the incurring of any liability. As Perritt explains:

> 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 tortfeasor 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.[31]

The nature and scope of the rights and responsibilities of the different persons involved in electronic communication depend not so much on their official role as on the amount of control and supervision they exercise, or are reputed to exercise, over the information and communications circulating in the open networks, or some part of them over which they have a certain control. Rendering some entity liable presupposes the possibility of identifying the persons who have control over the information in the various locations in this virtual environment.[32]

In this connection, Schlachter says:

> 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 or disseminate information. Also on this end are owners of private property, who are similarly protected from mandatory or forced access ... . At the other 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.[33]

This sliding scale does not concern only the rights of access to electronic environments, it also finds its full application in the field of liability. In this regard, Schlachter notes that 'Those entities with more editorial control generally also have greater exposure to tort liability for the statements or actions of others'.[34] This means that it is possible to classify the degree of liability on the basis of the degree of control which a person actually exercises over the information in a particular situation.

Editorial discretion: control over content Editorial discretion, mainly exercised by a publisher or broadcaster in the traditional environments, takes the form of discretionary editorial choices – the selection of the information to be published. It is the term denoting freedom of expression when applied to the media as entities.[35] Editorial discretion presupposes fundamental autonomy in decisions relating to the selection, treatment and circulation of information. However, its counterpart is liability: the holders of editorial discretion are liable *vis-à-vis* third parties for information circulated. Charkes explains below the close relationship between the principle of editorial discretion 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 judgement responsibility and, taken as a whole, will provide the public with necessary access to diverse views.[36]

Editorial discretion does not take into account the intention of communicating a message of a harmful nature. What counts is the intention of communicating a message whose harmful nature should have been known to the publisher.[37] Thus it is generally considered that the publisher is in a position to control all the information circulating in his or her medium of communication[38] and is liable for damages, and it matters little whether the offensive remarks are made by an employee, or in an open letter to the editor, or in an advertisement.[39] Liability for the transmission of information that may be illegal or harmful is a consequence of this power of control.[40]

Editorial discretion and its corollaries apply to any publication. However, whereas print media are free to undertake the publication of any text, the discretion of radio and television media, as broadcasters, is seen differently.[41]

Owing to the public character of the frequencies, the freedom of expression allowed to broadcasters is markedly more limited than that traditionally granted to the print media. However, the basic principle remains: the holders of a broadcasting licence enjoy editorial discretion even if it is more limited than in the other media. It has generally been held that broadcasting activities, unlike those of the print media, presuppose the use of a resource considered to be in short supply – that is, radio frequencies – which is regarded as constituting public property. Furthermore, the intrusive nature of the broadcasting media and their supposedly greater persuasive capacity have also been proposed as a justification for the special treatment of these media in regard to freedom of expression.[42] Despite these restrictions on editorial discretion, which take the form of an obligation to balance programmes and ensure that they reach a certain standard, it is posited that broadcasters incur liability as editors of the information broadcast by their organizations.

By contrast, the legal arrangements governing carriers reflect a total lack of editorial control. Carriers enjoy a special privilege which exempts them from liability for the content of messages carried by them on behalf of their users.[43] This follows from the fact that carriers are under an obligation to convey any message without discrimination, in terms of either the content of the message or the person sending it.[44] Carriers may exceptionally incur liability for the content conveyed if they are themselves the authors of the message, but they are not liable for content coming from third parties, for which they are merely a channel.[45]

Stratton Oakmont Inc. v. *Prodigy Services Co.*[46] was the first case in which a court found that a service provider exercised some editorial control, and recognized that it played an editorial role, as grounds for its liability. In this case, discussed earlier in the chapter, the New York Supreme Court, by classifying Prodigy as a publisher, held it liable for the damage caused to the defamed person. What is interesting in this judgment is that the Court, in order to classify Prodigy as a publisher, examined the latter's behaviour in regard to the information carried.

Physical control Actual physical control is exercised by a person who, knowing that he or she is contributing to the dissemination of a potentially harmful message, has the possibility of withdrawing the message and stopping its circulation, not by exercising editorial discretion over the content, but by withdrawing the material embodiment

of the content or the whole of the work. That such a factor is relevant to the incurring of liability stands to reason: 'an individual cannot incur liability for an unforeseeable and unavoidable act in respect of which s/he had no power to intervene.'[47]

Several examples taken from traditional communications contexts (press, radio, publishing) show that the possibility of effectively controlling the medium used to circulate the information may be one of the factors in the incurring of liability if the person implicated does not take the precautions available to remedy the harm done after publication or initial broadcasting.

In the field of online data transmission, it is considered that control presupposes preliminary preservation of the information in a medium:

> It must be realized, however, that these torts [defamation] presuppose preliminary preservation of the message in a medium. The idea is that the publisher has to control what is disseminated, but, as a counterpart, that s/he has to be in a position to do so ... . Now this point is extremely important from the angle with which we are concerned here, since a considerable part of the messages accessible on line, and hence their content, escape the service provider. The liability examined here is therefore incurred solely in the case of storage of the message (before it is made available to the public). And this irrespective of the duration: the person in charge of the service need only have been in a position to exercise the supervision expected of him or her by the law.[48]

Perritt stresses the fact that the possibility of exercising such physical control does not result solely 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.[49]

There is thus a close relationship between effective control over information and the extent of liability.

In the case of the liability of persons who participate in the transmission of messages over the Internet, the question then arises as to whether, in the event of damage, they were in a position to take effective action in regard to the information in order to prevent or limit the damage. To answer this question, one has to examine the possibilities of control over the information and the extent to which it is exercised. It is also important, however, to examine how far the persons concerned had knowledge of the information transmitted.

Knowledge of the Illegal or Tortious Nature of the Information

Knowledge of the harmful nature of a piece of information is closely related to a number of the factors on which liability is based. The question does not usually arise in the context of publishing, when knowledge of the harmful nature of the information goes together with a presumption of knowledge inherent in the exercise of editorial discretion: good faith on the part of the publisher does not make any difference to the liability incurred.[50] Publishing means communicating information to third parties, in the knowledge that it will be read, seen or heard. As a product of editorial discretion, publication presupposes a first-hand knowledge of the existence of the information transmitted.[51]

While editorial discretion entails a presumption of knowledge of the harmful nature of the information transmitted, in the absence of the exercise of such discretion, evidence of knowledge will have to be brought for liability to be incurred. Knowledge may be claimed in several circumstances:

> Knowledge, or the imputation of knowledge, can be established if the intermediary exercised content control over the messages on the network (for example 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 might 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.[52]

But how can it be made obligatory to prevent damage caused by the dissemination of information whose harmful or illegal nature is not likely to be established until after the hearing of both parties by a court? It is, after all, difficult for the administrator of an electronic mail server to decide as to the tortious nature of a message transmitted. The same question arises when the harmful nature of a piece of information is pointed out. What credence is to be placed on external sources of knowledge? And how should the information be subsequently reassessed?

These questions arose in an intellectual property context: *Religious Technology Centre* v. *Netcom Online Communication Services Inc.*[53] An anonymous user made available protected material of the Church of Scientology, through a discussion group. As soon as the Church was apprised of the infringement, it asked the system operator to withdraw the material. He refused to act until he had obtained additional evidence. The judge found that Netcom had incurred liability by its inaction, which was equivalent to substantive participation in the

illegal distribution of the material. However, this ruling does not provide useful guidance for a number of cases that occur in electronic communication. In the particular case on which the ruling was given, the evidence revealed that Netcom had done nothing to prevent the distribution of the *potentially* illegal material, having even refused to look at the material in question. But what weight must a notification have to place an obligation on the system operator, or any other intermediary able to prevent the damage by stopping circulation of the material, when it is the policy of the system operator not to exercise editorial discretion over the contents he or she helps to circulate?[54]

Another solution is to protect the intermediaries from all liability until a ruling is given as to the harmful, illegal or infringing nature of certain information whose circulation can be stopped. Perritt, however, points out the weaknesses in such an approach, in the case, *inter alia*, of the circulation of content infringing an intellectual property right:

> That approach would not adequately protect the interests of copyright holders. It takes a long time to get a judgement 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.[55]

The notion of knowledge is also dependent on the damage likely to be caused by the information. For instance, in the law of most countries, defamation has to result in the person defamed being perceived negatively by third parties – a criterion estimated in terms of the perception of an ordinary average person.[56] As soon as it is presumed that the exercise of editorial discretion entails the publisher's being in contact with the whole of the content published, it is taken for granted that the publisher, as a reasonable person, knew that the remarks with which he or she was in contact were likely to have an adverse effect on someone's reputation.

In the case of information of a factual character, it is difficult for intermediaries not involved in its production (as opposed to journalists, for instance) to know that it is inaccurate and hence likely to cause damage.[57]

Expertise

The notion of expertise is not exclusive to the field of information. It constitutes one of the chief criteria for the incurring of liability in various fields of activity. When an individual has recourse to an expert, the latter may be liable for certain specific obligations.

For instance, in the law governing building operations, some authors say that general contractors can incur liability for damages resulting from a building operation under their supervision in the absence of any specific negligence on their part, for it is considered that they guarantee that the building which they contracted to erect will be adequate and feasible, since it can be considered that the owner reasonably relied on the skill and judgement of the contractors.[58] Similarly, information brokers, although not themselves information providers, will incur liability if damage occurs as the result of information that is omitted, incorrect, out of date or incomplete:

> It is the fact that we are holding ourselves out as experts and being paid for specific expertise which creates the potential liability.[59]

Sookman goes still further, making explicit the close relationship between expertise and the dependence thereon of the recipient of the information:

> Where there is a contractual relationship between the information provider and the recipient of the information and the contract between the parties is silent as to scope of the duty of the information provider, if the former holds himself out as, or is known as, possessing some special knowledge, information or expertise in the field and furnishes information in that field to the recipient knowing that the recipient is likely to rely on the information, a legally enforceable duty to exercise reasonable skill and care in furnishing the information will be present.[60]

The concept of expertise may also apply in the field of knowledge, as noted by Elkin-Koren:

> In the context of copyright law, in order to guarantee full compliance a BBS operator would have to impose a high degree of monitoring. Proprietary rights are not an attribute of the text itself, but instead define a relationship among people concerning the work. Determining the status of proprietary rights in materials posted on a BBS thus would require further investigation. A BBS operator would have to determine in each case whether a subscriber copied or independently created a certain news text, poem or program. This places a heavy burden on BBS operators. Intellectual property involves a sophisticated body of law that is ambiguous with regard to digitized works. To understand this body of law requires a degree of expertise. Determining whether any particular work infringes copyright [also] requires some familiarity with the texts posted and the state of the art in that field.[61]

In the case of information of a technical character, the person with the expertise will often be the only one able to detect the erroneous nature of a piece of information and hence to remedy the situation – that is, to replace the potentially harmful data by accurate or appropriate data. That person's liability is then greater.

The Foreseeability of the Use of the Information and of the Damage

In a number of countries the notion of foreseeability is central to the establishment of norms of conduct, the reason being that the person referred to in provisions stating the rules governing liability is a 'reasonable and careful' person. The notion of foreseeability is therefore not only at the centre of the law of liability, it is also present in non-contractual liability for an act of information.

The criteria for the estimation of due care will be the likelihood of injury, the seriousness of the damage foreseeable and the burden of adequate protective measures. If serious injury is fairly likely, and the cost of taking the relevant measures is low, it will more readily be found that an obligation existed.[62]

According to Tiano, the likelihood and seriousness of damage have to be analysed on a case-by-case basis. The more dependent the user is on the provider, and the less control the provider has over the content of the information he or she transmits, the greater the likelihood of damage. Such an analysis may assist in foreseeing whether serious damage could reasonably be anticipated as a probable result of the acts and omissions of an information provider:[63]

> A duty of accuracy should not impose liability in every instance where inaccurate information is provided. Rather ... where the probability and gravity of foreseeable harm are great, the error reasonably preventable and the user's reliance on the information justified, a duty of accuracy should be imposed.[64]

The purpose of the information may also have a bearing on the foreseeability of damage. If the information can be used for only one purpose, the provider can foresee more exactly the damage that could result from that use. Spoor explains that:

> Much will depend on the kind of data and the ends which it may be expected to serve. A library catalogue is different from a database containing financial information, and still other standards should prevail for a medical database, the exactness of which may have a direct impact on patients' health and perhaps even their lives. ... The question whether data is sufficiently accurate or not cannot be answered without also considering what precision should reasonably be required, taking into account the expected use of the data.[65]

If the uses to which the information can be put are unlimited, the provider cannot foresee any damage which may result. In contrast, and to illustrate this point, it is reasonable to suppose that aeronautical information communicated to a pilot in a professional context is specific to a single use and a single type of user.[66]

The Role of the User

Liability for the transmission of erroneous information in a non-contractual situation is conditioned by the importance of the information to the recipient and the use that is likely to be made of it. Indeed, the liability of the persons implicated in the information chain is due largely to the fact that our society is increasingly dependent on information systems, and these systems, for their part, have a duty to be increasingly efficient.[67]

A user who is unfamiliar or unacquainted with the type of information communicated will be more inclined to rely on it and will have fewer reasons to check the veracity of the information conveyed.[68] Thus in *Fernand Nathan* v. *Gribinski*[69] (the hemlock case), the judge found that:

> No charge of negligence could be brought against the victim and her husband, both doctors of medicine but not specialists in botany, who had faith in the reliability of the X guide and could, without behaving irresponsibly, allow their daughter aged 14, an age of discretion, to use it. Nor could negligence be imputed to Mélanie Gribinski, who, on the basis of the statements in the guide, could have believed that the plant she was picking was harmless.

The more restricted the number of possible uses of a type of information, the more reasonable it is for the user to expect that information to be accurate (in so far as the information is used for the purposes for which it is supposed to be used).[70]

Despite the factor of reliance on the information communicated, it must also be noted that the role played by the user in the information transmission chain is not negligible. In this connection, Jérôme Huet says that:

> One may notice that often the role played by the user to whom the information is sent is often not at all neutral. The user is involved in the searches he does or, where he is a patient receiving long-term treatment, participates in the process by supplying data himself, so that it will often be a very delicate matter to untangle the original cause of the loss.[71]

It is therefore important to take into consideration even the way in which the user made the inquiry and/or made use of the information

obtained.[72] The user is also responsible for making appropriate use of the information.[73]

The Status of the Information Provider

Since electronic environments present a vast number of cases and the roles played by the persons implicated in the electronic information chain are diverse, it is imperative to take into consideration the different communication contexts in which information circulates.

The way in which the law of liability views communication situations varies according to whether the message is distributed to the general public or merely exchanged between two parties. In most legal systems, the law treats private conversation differently from the communication of information to the public. Furthermore, a vast number of locations for the distribution and exchange of information are to be found on the Internet and in other electronic environments. The term applied to them, bulletin boards, is very apt: users connected to a network post information on them so that it becomes accessible to all other users.

In cyberspace, everyone who is connected to the system can become an information provider. It would be inconceivable to assess the liability of the user who has a homepage on the Web without differentiating it from the liability of a large commercial business whose primary purpose is to supply the public with information. It is for this reason, moreover, that the law of most Western countries deals with messages by classifying them according to the context in which they were sent.[74]

The Accessibility of the Information

As in a paper environment, the data that a user receives must often be crosschecked to see whether they make sense.[75] The more possibilities there are of checking the accuracy of the data (for example, by means of legal data banks), the less justified and reasonable will be the user's reliance on their accuracy.[76]

> The very existence of damage will be likely to be disputed, in a case of the information service being unavailable, if the user had the possibility of applying to another source. The negligence of the user will often be put forward, particularly if it appears that the user should have checked the quality of the information supplied.[77]

It will no doubt be agreed that, generally speaking, a serious error that is difficult to detect should more readily incur the liability of the

intermediaries, whereas 'a slight error that is obvious and cannot escape detection by the user ... should not be sanctioned'.[78]

To summarize, the factors taken into account in the incurring of liability always concern the existence of real possibilities of preventing damage to one or other of the participants in electronic communication. The more a person involved is in a position to intervene and prevent or limit the harmful effects of the circulation of information, the more marked is the tendency to render that person liable.

REGULATION: HOW BEST TO APPORTION RESPONSIBILITY

Responsibility is a source of uncertainty: those who participate in communication in cyberspace do so more or less intensively according to whether they are or are not aware that they will have to assume responsibility for the information they send or help pass on. This conveys some idea of the importance of the mechanisms designed to apportion responsibility among the persons participating in cyberspace. The apportionment of responsibility among them, also the conditions under which they incur liability, are a consequence of the norms and regulations which apply in cyberspace and which constitute the source of the rights and duties of the persons participating in communication therein.

The different forms of regulation of electronic environments are in competition with one another.[79] Although national norms are currently the ones to which all those involved spontaneously refer, their legitimacy must not be taken for granted. Furthermore, despite the fact that alternative forms of regulation are increasingly gaining recognition, this does not necessarily signal that they will replace the national norms. According to Reidenberg, the hold of national governments is tending to weaken, but it will not cease to exist and should not be excluded as a matter of course:

> For global networks, governance should be seen as a complex mix of state, business, technical and citizen forces. Rules for network behaviour will come from each of these interest centres. Within this framework, the private sector must be a driving force in the development of the information society and governments must be involved to protect public interests. At the same time, policy-making cannot ignore technological concerns and technologically driven decision-making.[80]

Trotter Hardy, for his part, pointing out that the existing legal regime will continue to apply with regard to the issues it can deal with in electronic space, expressed the view that the issues specific to electronic environments would no doubt call for original solutions:

> Of course, a specific statutory response is only one of many legal reactions. Case-by-case adjudication and its common law build-up of precedents can also be applied to cyberspace legal issues as well; an international convention can enact uniform model laws; citizens can create their own customs; service providers can specify behaviour in their 'part' of cyberspace through contracts; a modest degree of anarchy may even be desirable.[81]

Such norms and regulations are conveyed by different means. They are sometimes embodied in international texts designed for application in all countries. In domestic law, constitutional provisions may lay down guidelines and principles as to what state law can do in connection with communication environments. In the United States, for instance, the First Amendment to the Constitution prevents the state from making any law which abrogates the freedom of speech or of the press. Such principles are often endowed with a long life. Owing to their 'supralegality', constitutional principles represent more than a mere technique of governance; they define the scope of the other rules that the state can introduce. On this account, they must necessarily be taken into consideration in any analysis of the regulatory techniques conceivable in respect of an information and communication phenomenon such as cyberspace. Furthermore, international and national norms are supplemented by a wide range of forms of regulation. Contracts, self-regulation, customs and practices, and sometimes even technology, all constitute different means of regulating the various activities connected with electronic environments.

This process of apportioning responsibility may assume a contractual form, as demonstrated by the many stipulations declining responsibility to be found in the contracts proposed by the Internet access providers. The apportionment of responsibility may often be defined in relation to national regulations, in order either to forestall or to anticipate some of their effects. First and foremost in the rule-making process, however, are the rules based on personal ethics and social pressure.

Personal Ethics and Social Pressure

The rules that have emerged so far to regulate the circulation of information on the Internet rest on the personal ethics of the users and are perceptible in communities sharing common aims or interests. Until now, rule-making has taken the form of self-correction by the members of communities of users. For instance, a piece of information disseminated by a web site may be the subject of feedback from someone located at any point connected with that site.

Information communities may develop generally accepted rules of conduct without the intervention of the law or state regulation. Internauts have arrived at rules in the interests of harmony in their relations with one another. These rules reflect the characteristics of this electronic environment.

Such cases of the spontaneous emergence of norms generally occur when there is a prospect of continuity in relations. Relations may be regular in certain contexts, such as networks of university researchers; they are much less so in the case of networks set up around more evanescent or more transitory interests. For this reason, the viability of an approach based solely on the rules of conduct adopted by the persons involved under the social pressure of just one particular electronic environment is open to question. Such rules usually appear in the presence of certain conditions, such as the need felt by the participants to continue to belong to a site observing certain rules.

On the other hand, it would be a mistake to dismiss too quickly the regulatory role of social pressure. Reference is often made to the practice of 'flaming'. Users dissatisfied or displeased with the behaviour of a participant at a site may inundate that person with sometimes insulting messages of protest. These practices reek of public obloquy, and the prospect of them suffices to encourage integrity on the network.

The desire to remain in an electronic environment may be enough to incline a number of protagonists to observe the rules that prevail there. The factors that appear to determine the extent to which norms of conduct are obeyed seem bound up with the individual's interest in remaining in a continuing relationship or one likely to be followed up. Is it not the normal reaction of any trader to behave in such a way that customers will want to come back?

While the regulatory effect of social pressure seems undeniable, it is nevertheless limited. It cannot, in isolation, ensure an efficient system regulating responsibility for information circulating in cyberspace.

Contracts

As electronic environments are primarily places for interaction, it is assumed that the protagonists want to be in contact. Apart from situations involving unsolicited electronic mail, interaction seldom occurs without a consensual move on the part of each of the protagonists. This shows the importance of contracts in the issue of the regulation of electronic environments.

Information is communicated over the Internet by means of a connection made deliberately by the user. It is therefore easier to see the

legal situation thus created as proceeding from a contractual relationship between transmitter and recipient. The fact that consent, or the option of withdrawing it, remain initiatives on the part of the user appears to be a key regulatory principle of the Internet. Nevertheless, while this contractual mechanism is appropriate for ensuring the protection of individual interests, it is not appropriate to the protection of necessary collective values.

Self-regulation

Self-regulation refers to norms that are voluntarily developed and accepted by those who take part in some activity. It is already widely practised in the sphere of the media and advertising. Use of the Internet reveals that several types of self-regulation are current.

For instance, webmasters may adopt policies in relation to access to the site, acceptable behaviour and prohibited acts. Most university institutions have established policies or rules defining the rights and prerogatives of those who make use of the institutions' information technology. These policies – sometimes made explicit in official documents or in the standard-form contract signed by the members or clients – relate to lines of conduct in matters such as the private character of e-mail, the conditions of use of the software available on the network, the obligation to use one's real name, the right to make public commercial announcements, the right to make use of the network's resources for personal purposes, and responsibility for the behaviour of subscribers or clients.

While the sanctions entailed by the non-observance of self-regulation are often only psychological, reproof may, in certain cases, be nevertheless very hard to endure. The Internet, in fact, gives wide publicity to unfavourable information: dissatisfied users can make people pay dearly for inappropriate behaviour.

National Law

Despite the obvious limitations to its effective application in some cases, national law may continue to apply in a great many situations resulting from the circulation of information on the Internet. A significant number of disputes implicate protagonists coming under the same national jurisdiction but, in disputes implicating protagonists coming under different national jurisdictions, the question of the application of the national law of a state arises in accordance with the principles of private international law. It is then a matter of determining which law is applicable and trying to obtain the sanction

of the law appealed to. The problem of applicability and of effectiveness is the same here as any private international law situation. A more serious problem arises in situations with regard to which national legislations contain public policy or morality provisions – for instance, what is obscene in one country may be quite acceptable in another. Indeed, each legal system reflects a slightly different cultural background, and the differences which can exist in national legislations further complicate the process of determining an appropriate body of rules to govern cyberspace. This may well lead to self-censorship in line with the policies of those countries which have the most restrictive systems of liability.

Even though networks are interconnected regardless of national frontiers, there are many circumstances in which a network will be considered, under state legislation, to be located on a particular national territory, so that someone can be rendered liable for what circulates in the environment over which the network is supposed to exercise control. It is therefore through the rules in regard to responsibility and liability that the law catches up with the protagonists.

It is naive to imagine that increasingly significant interaction can be developed in cyberspace without anyone being answerable for what goes on. So in the different national territories it is the most high-profile, and above all the most solvent, protagonists who are likely to take the rap for any offences committed in the electronic environments over which they exercise some control or which they help make available on a particular national territory. This encourages self-regulation. It is, indeed, in the interests of solvent protagonists to lay down rules to prevent matters getting out of hand and to avoid incurring liability for damages. Cyberspace communities, in accordance with their priorities and conceptions of the world, will have to set about promoting the emergence of a coherent and equitable legal framework to define the responsibilities of the participants in electronic communication.

CONCLUSION

It would be fitting to summarize the developments of this study by proposing an analytical interpretation of the rules and other factors determining responsibility as well as of the norms providing for its apportionment among the participants in electronic communication.

Determining the criteria for the apportionment of responsibility is a procedure which concerns all the participants in electronic communication as much as the authorities entrusted with making provision for the rules of conduct that are bound to govern the relations established in cyberspace.

In the early years of the Internet explosion it was possible to be content with asserting, by way of analysis, that the space created by the environments of interconnected networks transcended frontiers and afforded opportunities for evading regulations. Nowadays, it is important to go further and to acquire the means of establishing a set of norms appropriate to this environment. For this purpose, it must be recognized that the characteristics of cyberspace make it necessary to depart from the national paradigms which often predominate in any consideration of standard-setting in general, and of law in particular. The categories of law, as we know them, seem inadequate to cover all the rules essential to the smooth working of something as global and virtual as cyberspace. On the other hand, the fact that the laws of states can no longer be regarded as possessing a monopoly of the regulation of behaviour in this virtual environment does not mean that they are irrelevant: they will continue to play a major role when it comes to determining who is liable for tortious information.

To ensure equitable apportionment of responsibility, comparisons, but also the necessary distinctions, must be made between roles and functions in familiar communication contexts and those in cyberspace. It is also important to identify ways in which the values and precepts often proclaimed in international instruments should prevail in the apportionment of responsibility in electronic environments.

In short, it is more essential than ever to make a comparative evaluation of all the regulatory techniques in order to identify those most appropriate for bringing about the balances sought. Cyberspace law lags behind, not so much in the absence of rules covering certain incidents which may occur there as in the legal community's persistently confining itself to exclusively national paradigms when posing problems and establishing a basis for rules of conduct.[82] Yet in environments transcending frontiers, such as the high seas or airspace, it has long been known that the laws of states are only one aspect of regulation.

All the participants in electronic communication have a role to play in determining the principles of apportionment of responsibility. The protagonists need not wait for rules to come from the state. It is incumbent on them to define equitable precepts proactively in order to apportion the responsibilities to be assumed by the various participants in cyberspace activities. These precepts ought not to lie beyond the scope of the universally recognized principles concerning respect for human dignity and equality, and also for freedom of expression.

In any case, state authorities do not escape the obligation to ensure that their national legislations take due account of the balance between different fundamental values and adequately apportion responsibility among the various protagonists while respecting

fundamental rights. State authorities must ensure that the rules laid down by their legislation are adjusted to suit the new contexts of cyberspace.

NOTES

1 This study was carried out as part of a research project on the legal and regulatory framework of the new electronic environments undertaken by the Public Law Research Centre of the University of Montreal in 1995. This research was financed in the main by the Information Superhighway Fund of the Government of Quebec, with a supplementary subvention from the Social Sciences and Humanities Research Council of Canada. Fifteen researchers applied themselves to examining the principal legal aspects of cyberspace law and standard-setting with a view to making an initial summary of the law applicable to this sphere from a French-Canadian standpoint. The team, led by Pierre Trudel, comprised France Abran, Olfa Alani, Mylène Beaupré, Karin Benyekhlef, Athanasia Bitzkakidis, Luc Boucher, Sophie Hein, Fabienne Léonard, Eric Marcoux, Martin Michaud, François Quellette, Serge Parisien, Véronique Watiez-Larose and François Themens. An initial general study resulting from this research programme appeared in 1997 under the title, *Droit du Cyberspace*, Montreal, Editions Thémis, 1997. See http://www.droit.umontreal.ca/crdp/fr/texte/cyberspace/nv/nv001.html.

2 It is generally agreed that the word 'cyberspace' was coined by the author William Gibson in his novel, *Neuromancer*. Cyberspace, also called 'infosphere', is the virtual space of computers all linked up by means of networks explored by 'cybernauts' whose nervous systems are directly plugged in to the networks by means of 'plugs' fixed to their skulls. See G. Klein, 'De la cybernétique à la cyberculture', *Le Monde, Télévision, Radio, Multimédia*, 21–22 January 1996, p.28.

3 See J-C. Guédon, *La planète cyber Internet et cyberespace*, (Collection 'Découvertes', no. 280), Paris, Gallimard, 1996.

4 P. Lévy, *Cyberculture: Report to the Council of Europe*, Paris, Odile Jacob, 1997.

5 H.H. Perritt jr, 'Dispute Resolution in Electronic Networks Communities (The Congress, the Courts and Computer Based Communications Networks: Answering Questions about Access and Content Control)', *Villanova Law Review*, (38), 1993, pp.349ff. P. Trudel, F. Abran, K. Benyekhlef and S. Hein, *Droit du cyberespace*, Montreal, Editions Thémis, 1997, ch. 1. Also available at http://roma.crdp.umontreal.ca/crdp/chercheurs/trudelpar3/cyberspace/cnc/cnc010.html.

6 See P. Trudel and R. Gérin-Lajoie, 'La protection des droits et des valeurs dans la gestion des réseaux ouverts', in CRDP, *Les autoroutes électroniques: usages, droit et promesses*, Montreal, Editions Yvon Blais, 1995, pp.279ff at pp.306–7.

7 P. Trudel and R. Gérin-Lajoie, 'The Protection of Rights and Values in Open Network Management', in E. Mackay, D. Poulin and P. Trudel (eds), *The Electronic Superhighway: The Shape of Technology and Law to Come*, The Hague, Kluwer Law International, 1995, pp.159–92.

8 P. Trudel, 'Quel droit pour la cyberpresse? La régulation de l'information sur Internet', *Légipresse*, March 1996, pp.9–16; E. Schlachter, 'Cyberspace, the Free Market and the Free Marketplace of Ideas. Recognizing Legal Differences in Computer Bulletin Board Functions', *Hastings Community Enterprise Law Journal*, (16), 1993, pp.87ff. at p.100.

9 I. de Sola Pool, *Technologies of Freedom*, Cambridge, MA, Belknap Press, 1983,

p.2: 'America has had a trifurcated system of communications in which each mode, be it print, common carrier or broadcast, performed its specific function in ways unique to itself.'

10 T.A. Cutera, 'Computer Networks, Libel and the First Amendment', *Computer Law Journal*, (11), December 1992, pp.555ff. at p.581.

11 R.M. Neustadt, G.P. Skall and M. Hammer, 'The Regulation of Electronic Publishing', *Federal Communications Law Journal*, (33), Summer 1981, pp.331ff.

12 D.J. Loundy, *E-Law: Legal Issues Affecting Computer Information Systems and Systems Operator Liability*, 1995, http://www.leepfrog.com/E-Law/E-Law/Contents.html.

13 M.H. Ryan, *Canadian Telecommunications Law and Regulation*, Toronto, Carswell, 1995, p.416; L. Becker, 'Electronic Publishing; First Amendment Issues in the Twenty-First Century', *Fordham Urban Law Journal*, (13), 1984–85, pp.801ff. at p.857.

14 D.R. Johnson and K.A. Marks, 'Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?', *Villanova Law Review*, (38), 1993, pp.487ff. at p.495; Cutera, 'Computer Networks', op. cit., p.583. *Chastain* v. *British Columbia Hydro and Power Authority* [1973], 2 WWR 481; Law on telecommunications, LC 1993, c. 38, Article 36: 'Il est interdit à l'entreprise canadienne, sauf avec l'approbation du Conseil, de régir le contenu ou d'influencer le sens ou l'objet des télécommunications qu'elle achemine pour le public.'

15 T.C. May, 'Who is Responsible on the Net?', law.listserv.cyberia-l. Subject: Cyberspace is more like property, lease space, rent, etc. 7 February 1995. 12:31:21.

16 Ibid.

17 *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 NE 2d 160 (1970); *Tackett* v. *General Motors Corporation*, 836 F. 2d 1042 (7th Cir. 1987); *Woodling* v. *Knickerbocker*, 17 NW 387 (Minn. 1883).

18 Schlachter, 'Cyberspace, the Free Market and the Free Marketplace of Ideas', op. cit., p.118.

19 J.R. McDaniel, 'Electronic Torts and Videotext – At the Junction of Commerce and Communications', *Rutgers Computer and Technology Law Journal*, (18), 1992, pp.773ff. at p.825.

20 L.E. Becker jr, 'The Liability of Computer Bulletin Board Operators for Defamation Posted by Others', *Connecticut Law Review*, (22), 1989, pp.203–39 at p.217.

21 T. Arnold-Moore, 'Legal Pitfalls in Cyberspace: Defamation on Computer Networks', *Journal of Law and Information Science*, 5 (2), 1994, pp.165ff. at p.178. Also available at http://www.kbs.citri.edu.au/law/defame.html.

22 Johnson and Marks, 'Mapping Electronic Data Communications', op. cit., p.492.

23 Index No. 31063/94, NY Sup. Ct, 24 May 1995.

24 D. Loundy, 'Holding the Line, On-line, Expands Liability', *Chicago Daily Law Bulletin*, 8 June 1995, p.6.

25 Ibid.

26 T. Hardy, 'The Proper Legal Regime for "Cyberspace"', *University of Pittsburgh Law Review*, (55), 1994, pp.993–1055 at p.1003. Johnson and Marks, 'Mapping Electronic Data Communications', op. cit., p.493.

27 *Balabanoff* v. *Fossani*, 81 NYS.2d 732, 733 (Sup. Ct. 1948). US legal doctrine goes so far as to consider that a law imposing strict liability on distributors – a librarian, for instance – for the content of the works they distributed would be unconstitutional, since it would indirectly have the effect of restricting the information transmitted to the public (the works available being only those inspected by the librarian). See *Smith* v. *California*, 361 US 147 (1959), reh'g denied, 361 US Trotter Hardy, ibid.

28 Johnson and Marks, 'Mapping Electronic Data Communications', op. cit., p.493.
29 *Cubby Inc.* v. *Compuserve Inc.*, 776 F.Supp. 135 (*SDNY*, 1991), p.140. Also available at http://www.jmls.edu/cyber/cases/cubby.txt; http://www.leepfrog.com/E-Law/Cases/Cubby_v_Compuserve.html; http://ww.cpsr.org/cpsr/free_speech/cubby_v_compuserve.
30 McDaniel, 'Electronic Torts and Videotext', op. cit., p.823.
31 H.H. Perritt, jr, 'Tort Liability, the First Amendment and Equal Access to Electronic Networks', *Harvard Journal of Law and Technology*, (5), 1992, pp.65ff. at pp.110–11.
32 Trudel, and Gérin-Lajoie, 'La protection des droits et des valeurs', op. cit., pp.324–5.
33 Schlachter, '*Cyberspace, the Free Market and the Free Marketplace of Ideas*', op. cit., pp.113ff.
34 Ibid.
35 S.D. Charkes. 'Editorial Discretion of State Public Broadcasting Licensees', *Columbia Law Review*, (82), 1982, pp.1161ff. at p.1172.
36 Ibid.
37 McDaniel, 'Electronic Torts and Videotext', op. cit., pp.817–18.
38 Johnson and Marks, 'Mapping Electronic Data Communications', op. cit., p.492; R. Beall, 'Notes: Developing a Coherent Approach to the Regulation of Computer Bulletin Boards', *Computer/Law Journal*, (7), pp.499ff. at p.505.
39 Johnson and Marks, 'Mapping Electronic Data Communications', op. cit.
40 Ibid.
41 F. Jongen. 'La liberté d'expression dans l'audiovisuel: liberté limitée, organisée et surveillée', *Revue trimestrielle des droits de l'homme*, 1993, pp.95ff; M. Dejeant-Pons, 'La jurisprudence en matière de liberté d'expression audiovisuelle dans le cadre de la Convention européenne des droits de l'homme', in C. Debbasch and C. Gueydan, *La régulation de la liberté de la communication audiovisuelle*, Paris, Economica, Presses Universitaires d'Aix-Marseille, 1991, p.285; A. Namurois, 'Aspects du droit de la radio et de la télévision dans le monde, en rapport avec la liberté d'expression', *Etudes de radio-télévision*, **27**(1), May 1980; M. Fallon, 'La radio et la télévision face au juge européen', *Annales de droit de Louvain*, (47), 1987, p.153; S.W. Head, *World Broadcasting Systems – A Comparative Analysis*, Belmont, Wadsworth, 1985, pp.377ff; D. R. Browne, *Comparing Broadcast Systems*, Ames, Iowa State University Press, 1989.
42 P. Trudel and F. Abran, *Droit de la radio et de la télévision*, Montreal, Editions Thémis, 1991, pp.153ff; A.C. Evans, 'An Examination of the Theories Justifying Content Regulation of the Electronic Media', *Syracuse Law Review*, (30), 1979, pp.871ff at p.884.
43 Ryan, *Canadian Telecommunications Law and Regulation*, op. cit., p.416. Becker, 'Electronic Publishing', op. cit., p.857.
44 Johnson and Marks, 'Mapping Electronic Data Communications', op. cit., p.495; Cutera, 'Computer Networks', op. cit., p.583; *Chastain* v. *British Columbia Hydro and Power Authority* [1973] 2 WWR 481; *Loi sur les télécommunications*, LC 1993, Ch. 38, Art. 36: 'Il est interdit à l'entreprise canadienne, sauf avec l'approbation du Conseil, de régir le contenu ou d'influencer le sens ou l'objet des télécommunications qu'elle achemine pour le public.'
45 F. Abrams and D. Ringle. 'Content Regulation (Symposium: Legal Issues in Electronic Publishing)', *Federal Communications Law Journal*, (36), September 1984, p.153.
46 Index No. 31063/94 NY Sup. Ct, 24 May 1995, http://www.customs.com/prodigy2.html.
47 N. Vallières and F. Sauvageau, *Droit et journalisme au Québec*, Quebec, Editions GRIC-FPJQ, 1981, pp.25–6.

48 M. Vivant (ed.), *Lamy droit de l'informatique: informatique, télématique et réseaux*, Paris, Lamy SA, 1996, p.1206, No. 1893.
49 Perritt, 'Tort Liability', op. cit., pp.110–11.
50 J-L. Baudouin, 'La responsabilité causée par les moyens d'information de masse', *Revue juridique, Thémis*, 1973, pp.201ff.
51 Becker, 'The Liability of Computer Bulletin Board Operators', op. cit., p.217.
52 Perritt, 'Tort Liability', op. cit., p.107.
53 907 F. Sup. 1361 (ND Cal. 1995).
54 'The Scientology Lawsuits and Lawyer Letters: The Problem Faced by On-line Services Who Get Notice of Users' Alleged Violations', *Legal Bytes*, **4**(1), Spring 1996. Also available at http://www.gdf.com/1b4-1.htm.
55 H.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.
56 N. Vallières, *La presse et la diffamation*, Montreal, Wilson & Lafleur, 1985, p.20.
57 J.H. Spoor, 'Database Liability: Some General Remarks', *International Computer Law Adviser*, (3), April 1989, pp.4–6: 'It may well be argued that the producer will be liable if he publishes or fails to correct inaccurate data after he discovers they are 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.'
58 W.H.O. Mueller, 'Responsibility of Contractors and Project Managers for the Defective Design of Building Components and Systems and Exclusion of Insurance Coverage for this Risk', *Connecticut Law Review*, 1986, pp.103ff.
59 T. Pritchard, 'The Information Specialist: A Malpractice Risk Analysis', *Online*, **13**(3), 1989, pp.57ff; J.A. Gray, 'Personal Malpractice Liability of Reference Librarians and Information Brokers', *Journal of Library Administration*, **9**(2), 1988, pp.71ff.
60 B.B. Sookman, 'The Liability of Information Providers in Negligence', *Computer Law and Practice*, **5**, 1989, pp.141ff.
61 N. Elkin-Koren, 'Copyright Law and Social Dialogue on the Information Superhighway: The Case against Copyright Liability of Bulletin Board Operators', *Cardozo Arts and Entertainment Law Journal*, **13**, 1995, pp.345ff. at p.405.
62 B.R. Bawden, 'Les dix commandements de l'informatisation: l'obligation de diligence face à l'usage de la technologie, *CA Magazine*, **126**(34), August 1993, pp.34ff.
63 J.R. Tiano jr, 'The Liability of Computerized Information Providers: A Look Back and a Proposed Analysis for the Future', *University of Pittsburgh Law Review*, **56**, 1995, pp.655ff. at p.687.
64 Ibid., p.676.
65 Spoor, 'Database Liability', op. cit., p.6.
66 Tiano, 'The Liability of Computerized Information Providers', op. cit., p.683.
67 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', *Tulane Civil Law Forum*, **5**, 1990, pp.101ff. at p.127.
68 Tiano, 'The Liability of Computerized Information Providers', op. cit., p.684.
69 Paris Court of Major Jurisdiction, 29 May 1986, RTD civ. 1988, p.365.
70 Tiano, 'The Liability of Computerized Information Providers', op. cit., p.683.
71 J. Huet, 'Liability of Information Providers', op. cit., pp.108–09.
72 Vivant, *Lamy droit de l'informatique*, op. cit., p.460, No. 719. As faulty equipment may contribute to faulty data, users are also responsible for the correct functioning of their electronic equipment: B. Tarter, 'Information Liability. New Interpretations for the Electronic Age', *Computer/Law Journal*, **11**, 1992, pp.481ff. at p.530.

73 Ibid., p.532.
74 Trudel and Gérin-Lajoie, 'La protection des droits et des valeurs', op. cit., p.317.
75 Tarter, 'Information Liability', op. cit., p.532.
76 Tiano, 'The Liability of Computerized Information Providers', op cit., p.684.
77 J. Huet and H. Maisl, *Droit de l'informatique et des télécommunications*, Paris, Litec, 1989, p.637, No. 579.
78 L. Sabater-Bono, 'Banques de données: la responsabilité des informations', *Expertises*, (98–99),1987, pp.309ff at p.316.
79 Trudel et al., *Droit du cyberespace*, op. cit., ch.3.
80 J. Reidenberg, 'Governing Networks and Cyberspace Rule-Making', *Symposium on Information, National Policies and International Infrastructure*, Harvard, 28–30 January 1996, at http://ksgwww.harvard.edu/~itbspp/reidpap2.htm. The author goes on to say: 'State governments can and should be involved in the establishment of norms for network activities, yet state governments cannot and should not attempt to expropriate all regulatory power from network communities.'
81 Hardy, 'The Proper Legal Regime for "Cyberspace"', op. cit., p.995.
82 Trudel et al., *Droit du cyberespace*, op. cit., pp.cnc 1 to cnc 8.