8.0 Introduction

In the simplest terms, to be an intermediary is to be like a conduit for the passage of any information/communication. For e.g., your post-man is a sort of an intermediary between the sender and you. Of course, you know that your post-man does not change or alter the message, neither does he open it or modify in it in any way and delivers it to you as it is received by him, from the sender. Neither does he derive any benefit that is related to the delivery of such messages, apart from a fixed emolument. Similarly, an intermediary in the digital world is one which acts as a conduit through which information passes through and communication is enabled. Network service providers, Internet service provider, web hosting providers are all examples of intermediaries. Worldwide, the law on intermediary liability has evolved in a manner, which grants liability to intermediaries, if it plays the role of a “perfect conduit”, like that of the postman mentioned above, where an intermediary merely acts as a facilitator or transmitter of information/communication.

There are numerous players acting in the Internet world; some are totally separate commercial entities, and some are part of the same corporations. One of the most known is America On-Line (AOL),\(^1\) which plays several roles, such as access provider, host service provider, information location tool provider, and even content provider. The different roles played by the on-line intermediaries may affect the liability regime applicable. Thus, focusing attention on the different roles that the on-line intermediaries play within cyberspace, the following entities can be described:

a) Network operator: providing the technical facilities for the transmission of information.

b) Access provider: providing users with access to the Internet.

---

\(^1\)AOL is the leading internet access provider in the U.S. and the only provider with apan-European presence. In Europe AOL operates mainly through two joint ventures: AOL Europe, a 50/50 deal with Bertelsmann, and AOL CompuServe France, a venture with both Bertelsmann and Vivendi subsidiaries Cegetel, and Canal Plus. See AOL Time Warner, Corporate Information, at http://www.aoltimewarner.com/corporate-information/index.adp.
c) Search Engines: on-line tools used for finding Web sites such as Yahoo!, AltaVista, Google, etc. There are two types of search engines, namely, "automated" search engines and search engines that rely upon people to review and catalogue Web sites.

d) Host service provider: services in which users may rent Web site space, set up Web pages, and upload content, such as software, text, graphics, or sounds. Hosting services may include on-line exchanges also, like bulletin boards and chat rooms.2

Bulletin board and news group users can read information sent by other users and post their own messages. Usually, bulletin boards, news groups, and chat rooms are devoted to specific topics.3 Chat rooms allow users to exchange files and communicate in real time with each other. It is a more interactive service that also allows for file exchange.4 To be able to gain exemption from liability for any violation caused because of the information transmitted, an intermediary must generally not:-

1) Originate a communication of an information by itself or,
2) Select by itself, the originator or the recipient of the communication or,
3) Alter or modify the content of the communication.

On the foundation of such broad principles largely, the liability of an intermediary is determined with its attendant differences (the devil in the details) as is the case with different municipal laws among nations.

8.1 ISPs' liability in the United States

In the United States, one of the Acts which provides the liability for the ISPs is the Digital Millennium Copyright Act 1998. This Act governs the liability of the Internet sites and ISPs for the copyright infringement of its user. It provides a mechanism for copyright owners to force site owners and ISPs to remove infringing material. For

---

3Id at 4.
4It is much more difficult to detect copyright infringement in files exchanged in a chatroom than, for example, on a web page that displays a permanent link to static files.
example, You-Tube which is an ISP as restricted by the Act have the right to remove any illegal post or unauthorized copy that are posted from its site.

The following elements are part of the regime under the DMCA:

1) The online service provider [hereinafter OSP] must have a designated agent to receive notices and it must use a public portion of its Web site for receipt of notices;

2) The OSP must notify the U.S. Copyright Office of the agent’s identity and the Copyright Office will also maintain electronic and hard copy registries of Web site agents.5

When discussing about the liability for the ISPs, some of the cases which can be referred is the Netcom case and Sega Enterprises v. Maphia. These two cases are quite relevant to our topic which concerned the nature of You-Tube. In the Netcom case, the court held that the ISP is only liable for the contributory infringement and not under the direct infringement as the ISP uses an automatic pass-through of allegedly infringing messages posted by its subscriber. To pass under the contributory liability, the court decided that there must be a direct infringement, to which the contributory infringer, which in this case was Netcom, has knowledge and encourages or facilitates the illegal act. The court in the subsequent Sega v. Maphia case held that a BBS (Bulletin Board Service) and its system operator liable for contributory infringement for both the uploading and the subsequent downloading of copies of Sega’s video games by users where the system operator had knowledge that the infringing activities was going on through the bulletin board. In Sega’s case, the claim under direct liability was also refused by the court on the basis that the operator (Maphia) had not participated in the very acts of uploading or downloading themselves.

The element of knowledge must also be fulfilled to succeed under this claim. If the operator does not have any knowledge about the infringing materials post on its site, no liability can be charged upon the ISPs. In short, the requirement of knowledge may eliminate contributory liability on the part of ISP or BBS operator with respect to many 

---

instances of infringement for which ISP or BBS merely a passive information conduit and has no knowledge of the infringement.

8.2 Liability of Intermediary Service Providers in European Union

8.2.1 Preliminary Concepts

There are two approaches to deal with the liability of an ISP. In a vertical approach, different liability regimes apply to different areas of the law. This is the approach adopted by the United States. The Digital Millennium Copyright Act deals with copyright issues, whereas the Telecommunications Act of 1996 deals with liability derived from violations of other types of laws. In a horizontal approach, there is one liability regime applicable to any infringement regardless of the area of law. Thus, the same regime will be applicable to any type of infringement, whether it is copyright, defamation, or privacy rights. The horizontal approach is used by the EU Directive. It is argued, that a horizontal approach is favorable because ISPs do not have to monitor the content of the material published by their customers. If the EU had adopted a vertical approach that applied different legal liability regimes to the data flowing through the systems, ISPs would have been obliged to decode the bits that form the data and analyze all the content (music, images, etc) before posting. This would have been an extremely weighty burden to place on the ISPs' shoulders, with the possibility of converting them in censorship agents.

The Directive does not establish a general liability regime applicable to ISPs. Instead, it provides for a system of specific liability exemptions. This means that in cases where the ISPs provide a specific service (mere conduit, caching, and hosting) and comply with a series of requirements, they will not be held liable for the services

---

6Julia- Barcelo, supra note 2, at 15.
7See DMCA, supra note 5, Julia- Barcelo, supra note 2, p.16.
10Julia- Barcelo, supra note 2, p.15
performed (within some limitations). The limitations apply only to liability for damages because the last paragraphs of Articles 12, 13, and 14 of the Directive establish that Member States retain the right to require the ISPs to terminate or prevent known infringements. Moreover, it is stated in Recital 45 of the Preamble that the limits on the liability of ISPs includes injunctions of different types and court orders that require the "termination" or "prevention" of any infringement. This includes prohibitory injunctions, where the ISPs are required to desist from wrongful activity, and mandatory injunctions, where ISPs are required to rectify any wrongdoing. It must also be kept in mind that the Directive only provides for a system of liability exemptions for ISPs. Thus, if an ISP does not qualify for an exemption under the Directive, its liability will be determined by the national laws of the respective Member States. Additionally, even when it is known that ISPs can undertake different activities, the Directive liability distinctions are based on different categories of services provided by the ISPs, rather than on different categories of services providers.

8.2.2 Activities of the ISP Covered by the Directive

It is important to emphasize that all on-line activities must be in contact with at least one ISP; therefore, it is important to have a clear way to avoid uncertainty when dealing with ISPs. There are different ways to accomplish this. One way is to set up an objective exemption for specific activities. An objective exemption could provide freedom from liability for ISPs engaged in activities predetermined by the legislature as permissible. The Directive provides an objective exemption for ISPs engaged in "mere conduit" activities, as long as they have complied with the Article 12 requirements. For "caching" and "hosting" services, the Directive provides subjective exemptions. The applicability of subjective exemptions rests upon whether the ISP, in addition to complying with the objective criteria from Article 12, has complied with additional due diligence requirements.

1. Mere Conduit

Article 12 provides for two types of "mere conduit" activities. The first consists of "the transmission in a communication network of information provided by a recipient of

12Julia-Barcelo, supra note 2, at 8.
the service. The ISP is playing a passive role in such activities by acting as a mere "carrier" of data provided by third parties through its network. The second type of mere conduit activity is commonly known as "providing Internet access." Mere conduit activities include the automatic, intermediate and transient storage of the information transmitted, in so far as it takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

This provision describes the process of "packet switching transmission," which allows ISPs to store information for a shorter period of time in small pieces. The packet switching transmission process allows ISPs to provide mere conduit activities by making copies of the information for the sole purpose of carrying out the transmission of the information, without making the information available to subsequent users. The term "automatic" refers to the fact that the act of storage occurs through the ordinary operation of the technology. As interpreted by the government of the United Kingdom, the term "intermediate" means that the "storage of information is made in the course of the transmission," and the term "transient" refers to the fact that "the storage of the information is temporary and not to be stored beyond the time that is reasonably necessary for the transmission.13

When ISPs meet the conditions established in Article 12, their standard of liability is "no liability." This is because they have no control over the data flowing through their network. The ISPs cannot be held liable for the information transmitted as long as they do not perform the following steps:

1) Initiate the transmission; i.e. the provider does not make the decision to carry out the transmission. The fact that a provider automatically initiates a transmission at the request of a recipient of its service does not mean that the service provider initiated the transmission.14

2) Select the receiver of the transmission; applicable when the ISP selects receivers as an automatic response to the request of the user initiating the transmission. This includes forwarding e-mail to a mailing list, at the request of the recipient.

14Directive, supra note 11, at art. 12(0)(a).
3) Select or modify the information contained in the transmission; not including manipulations of a technical nature which take place in the course of the transmission, since such manipulations do not alter the integrity of the information contained in the transmission.

2. Caching

The purpose of a caching service is to avoid saturating the Internet with the repetitive high demand of certain material. ISPs decrease this demand-overload by locating the high demand data on remote servers, then storing copies of the material on local servers. This allows delivery to information seekers in the quickest way, because the data has less distance to travel to reach end-users. This automatic, intermediate, and temporary storage of data in local servers is called "caching" for the purposes of the Directive. Other types of caching, such as long-term caching, are not included in the Directive and therefore are not included in the liability exemptions. ISPs cannot be held liable when they perform caching on the condition that:

1) The provider does not modify the information;

This is the basic condition to be held not liable. The rationale behind the exemptions is namely that the ISPs respect the content that their clients post on the Web in its entirety. Otherwise, the ISPs could be held liable, even when they did not create the information. The provider complies with conditions on access to the information;

This means that the conditions on access to the original data should be respected for the cached copies as well. Sometimes, the original party posting the information applies certain conditions to access; for example, a subscription fee for entering specific data. Accordingly, when the provider accesses the information for caching purposes, it must comply with the access requirements in place (plus, the following conditions), in order to avoid liability.

2) The provider must comply with rules regarding the updating of information, specified in a manner widely recognized and used by industry;

3) The professional codes that deal with the update of the information must be used by the providers. This is important especially when the information that is cached

---

is otherwise updated frequently, as in the case of personal information or scientific or economic information that must be very precise;

4) The provider must not interfere with the lawful use of technology that is widely recognized and used by industry to obtain data on the use of the information; and

5) The provider must act expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

There are several situations under this last sub-requirement in which the provider cannot be held liable:

1) The provider must allow the original Web owner or creator to get the information regarding the Web page access, i.e. from where and from whom the hits to his Web page come (that in this case will be to the cache copy instead of the original Web page). The provider generally acts expeditiously to remove or disable access to information it has stored, upon obtaining actual knowledge that at the initial source has been:
   a) removed from the network;
   b) access to the information has been disabled; or
   c) A competent authority has ordered the removal or disablement of the information.

Receipt of actual knowledge can often occur through a simple process. To begin with, it is important to keep in mind that Article 15 prohibits Member States from compelling ISPs to monitor the information which they transmit or store. Thereby, the actual knowledge requirement must be interpreted in light of Article 15. That is to say, ISPs obtain actual knowledge if they receive the information from a third party, but not from their own inquiry upon the content of the information stored. After having received the information concerning the three conditions of the original Web page, the ISPs must act promptly to remove the materials from its network.
3. Hosting

One key to success for the Internet is the opportunity for any individual to rent space from a host provider, where that individual may post any kind of material, at any time and at a very low cost sometimes even for free. This rent can also be provided through bulletin boards and chat rooms. "Hosting," therefore, defines the service that provides offers to individuals, companies, and organizations to rent space and incorporate any kind of data on the space.16 ISPs will not be held liable for performing this activity as long as,

1) the provider does not have actual knowledge of illegal activity or information and, as regarding claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

2) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

It is also provided that the abovementioned shall not apply when the customer of the service is acting under the authority or the control of the provider. This reinforces the raison d’Otre behind the limitation of liability, namely that ISPs may be held liable if they have some form of "control" over the information.

Thus, mere knowledge or awareness of illegal activity alone is not enough alone to make a host provider liable, especially if the ISP acts promptly to remove the information or to disable access to it. Now, the problem of determining the precise meaning of actual knowledge reemerges.17 The Directive does not establish a "notice take down" regime, as is found in the Digital Millennium Copyright Act (DMCA) in the U.S.

Proper written notification from a copyright owner to an OSP must include:

1) the name, address and electronic signature of the complaining party,

2) sufficient information to identify the copyrighted work or works,

3) the infringing matter and its Internet location, a statement by the owner that it has a good faith belief that there is no legal basis for the use of the materials complained of, and

4) a statement of the accuracy of the notice and, under penalty of perjury, that the complaining party is authorized to act on behalf of the owner.

The only analogous provisions appearing in the Directive are found in Articles 14.3 and 21.2. Article 14.3 leaves Member States with the discretion to establish "notice and take down" procedure; and Article 21.2 provides that, when the Directive is next re-examined, the issues to be analyzed will include the notice and take down procedures and the attribution of liability following the taking down of content.

This lacunae in the Directive poses several problems. First and foremost is that ISPs would not be able to know whether they are properly informed, whether the information received is founded or not and whether they can face liability claims for Web page creators when their pages have been shut down. This is especially the case if it has been proven that the content was neither illegal nor harmful. Consequently, a clear and detailed mechanism should be established that balances the competing interests at stake.

Whereas copyright holders have the right to protect their materials, Web creators have the right to express freely without a permanent threat of being removed or disabled after an unfounded complaint has been received by the host provider, and the host providers have the right to have predetermined guidelines that allow them to know whether to disable access to a Web page or not. Even if tough specific requirements for the notices of copyright infringements are established, the risk of an unfounded claim cannot be totally ruled out. It is therefore necessary to set up the so-called "put back procedure." It is possible through such a procedure to obtain more complete protection for all the actors involved, as well as a proper balance between freedom of expression and fair competition. Through this mechanism, a person whose Web page has been disabled has the right to request its replacement or re-posting. If this request is made in compliance with the guidelines, then the host provider has to restore access to the Web page. If a court action is then filed for the removal of access to the material from the host provider site, the ISP must do so. It has been submitted however, that within the European framework it would be better to decide that an ISP should disable access only if a court injunction is issued.

Finally, it is worth considering what type of liability is imposed upon the sender of unfounded notices to ISPs which lead to the removal of material. Under the DMCA liability is imposed to the person who sends an intentional false notification. There is no provision concerning this issue in the E-commerce Directive. As a result, national liability laws will apply. And because in most of these laws liability is based on fault, only when national courts finds that the sender was aware of the lack of proper grounds to send the notice leading to the take down of content will he be held liable.

8.2.3 No General Obligation to Monitor

Article 15 of the Directive states that Member States shall not impose a general obligation on providers to monitor the information they transmit or store when they are performing one of the services analyzed above, namely mere conduit, caching, and hosting, and also cannot compel them to seek facts or circumstances indicating illegal activity. Basically, a general obligation to monitor the information cannot be imposed on providers under the Directive. This is very reasonable since such an obligation could render it almost impossible to provide services in a realistic and commercial way, if providers were obliged to check and control all the information that flows through their networks. In its second paragraph, Article 15 establishes a more specific obligation for ISPs. The ISP is obliged "to promptly inform the competent public authorities of alleged illegal activities" or information provided by the ISP's customers, or to "communicate to the competent authorities," at the request of the authorities, information that enables the identification of those customers with whom the ISP has a storage agreement.

This paragraph imposes a duty of communication from the ISPs to the competent authorities in the case of suspected illegal activities. It is assumed that Member States, when implementing this provision, shall take into account the proper legal judicial guarantees in order to balance all the rights at stake, namely the investigative rights of the Member States' organizations, versus the privacy and freedom of speech rights of the recipients of the ISPs services. For instance, in Spain, the proposal for the transposition of the January 18, 2001
Directive in this area establishes that the ISPs, in relation with their content, have the following disclosure obligations:

1) to communicate to the judicial or administrative competent authorities, when they have knowledge that the alleged illegal activity performed by the recipient of the service; and

2) to communicate to the judicial or administrative competent authorities, at their request, the information that allows for the identification of the recipient of the services.

In relation with the provisions of Article 15.2 of the Directive, the Spanish proposal provides that "the competent judicial authority can request to any ISPs to supervise or to keep all the data related to a determined Web site for a maximum of six months and to put it available to the authority." As is seen in this proposal, judicial authorities are called to act in order to protect the rights of all parties involved. However, the statutory approach in relation to the duty of communication established by Article 15.2 has not been adopted by all Member States.

8.2.4 Directive Loopholes

The EU Directive falls somewhat short in some areas, specifically, in the Directive's coverage of the notice requirement and procedure for blocking content, freedom of expression, and unfair competition. Many concerns arise through the automatic imposition of liability on ISPs for the removal of content, as well as liability for information tool services [hereinafter ITS]. Since the first of the two have been addressed above, the focus in the latter portion of this Article now turns to ITS liability.

8.2.4.1 The Liability of Information Tool Services

The ITSs, which include "search engines," are one of the most important actors in the everyday development of the Internet. They allow users to find information in a network that is exponentially increasing its number of pages on an annual basis. ITSs perform their activities in two ways. The first is the creation of databases with Websites arranged by thematic, geographic, or some other criteria that facilitate users in finding the

---

sought-after data. Through user-entered prompts, ITSs also display lists of Web pages with requested information. For example, a user entering a search string using the term "electronic commerce," is presented with a list of Web pages containing at least one of the two words. However, if you want to narrow your search only to "electronic commerce in Italy," then only Web pages with at least one of these three words will appear. The list of Web pages consists of links included in the "search result" page of the ITS.

The next question that must be addressed is whether it is reasonable to impose liability upon an ITS that links to Web pages containing unlawful material. Is it reasonable to expect an ITS to know or have some reason to believe that any of the millions of Web pages that normally appear on the "search results" Web page could include illegal material? Or, in other words, it is reasonable to impose a duty of care on ITSs in order to control all the material that they provide, in an indirect way, through the links they display? To answer these questions, it should be explained very briefly how an ITS typically works. The indexing and searching functions are normally performed either by robots or by human beings.20 It is obvious that the former cannot distinguish by itself whether a Web page contains illegal material. On the other hand, it can be argued that a human being can do so quite easily. However, it must be kept in mind that human indexers of Web content typically work in a similar fashion to persons who index huge paper-based libraries; they only have time to take a quick glance at the Web pages to determine into which category the pages should be indexed. Therefore, it may be impossible for even human indexers to determine in a few seconds whether a certain Web page is displaying illegal material.

In the U.S., the DMCA has incorporated a liability limitation for the ITS's acts of linking users to a site containing infringing material, as long as the following conditions are met:

1) the provider must not have the requisite level of knowledge that the material is infringing if the provider has the right and ability to control the infringing activity, the provider must not receive a financial benefit directly attributable to the infringing activity; and

2) upon receiving notification of claimed infringement, in the form of a proper notice, the provider must expeditiously take down or block access to the allegedly infringing material.

In light of the abovementioned considerations, it is possible to outline the basic principles of liability exemptions that should be granted to ITS. First, ITSs should not be held liable for merely providing a link to a site containing illegal material, whether it is the product of a human or robot indexing function. Real persons have insufficient time to discern the character nuances of Web pages, and programmers likewise do not have the time or resources to design automated robots to filter out all illegal content. The scope of liability exemptions must cover both human and robot search engines. Additionally, ITSs should only be held liable in the case where they are well aware of the illegal content of a Web site indexed on their Web pages. This "awareness" requirement should be satisfied by "proper and complete" notice given by interested parties to an ITS, in the same manner as required under the DMCA. With these main provisions, the legal uncertainty that ITSs currently face could be avoided, in so far as the possible outcome of a complaint filed against an ITS for providing links to illegal material would be avoided.

8.3 The Position in Australia
8.3.1 The Earlier Position

The position in Australia cannot be answered without reference to the case of Telestra Corp. Ltd. v. Australasian Performing Right Assn. Ltd.\textsuperscript{21} Although this case does not involve ISPs; the decision holds much significance for them. In Telestra, the plaintiff played music owned by the defendant to the plaintiff's clients while they were placed "on hold" on the telephone. Here, the court agreed with the defendant that the transmission of another's work through a diffusion service, infringed the defendant copyright owner's rights. The concept of a Diffusion Right is paramount in Australian law and is also used in judging claims against ISPs.\textsuperscript{22}

In order to come under the purview of the diffusion right, three elements must be satisfied:

\begin{itemize}
\item \textsuperscript{21}(1997) 38 I.P.R. 294.
\item \textsuperscript{22}(1997) 38 I.P.R. 294.
\end{itemize}
1) There must be a diffusion service. Diffusion involves "the transmission of the work or other subject matter in the course of a service of distributing broadcast or other matter over wires, or other paths provided by a material substance." The music transmitted over the telephone in Telestra, amounted to such a diffusion service.

2) The work must be transmitted to the subscribers. In Telestra, the subscribers to the telephone service were deemed to be subscribers to the diffusion service, because clients who used the telephone service were placed on hold and could receive the music transmission.

3) The alleged infringer must cause the transmission of the allegedly infringed material. In Telestra, the person operating the service is deemed to be the "person causing work to be transmitted. "The "person who undertakes to provide the service to subscribers in agreements with them," is taken to be "the person operating the service."

Therefore, all three elements were satisfied, and the court held Telestra liable for the infringement.

Next the Australasian Performing Rights Association, Limited (APRA), filed suit against a leading Australian ISP, OZE mail, that was settled soon thereafter. Based on the decision in Telestra, the ISP would most likely have lost because all the three elements of Section 31(1)(a)(v) were present. The ISP involved a diffusion service, it transmitted the works to the premises of the customers, and pursuant to the contract between the customer and the ISP, the ISP provided a service to the customer. The ISP therefore became the entity that caused the transmission.

8.3.2 The Copyright Amendment (Digital Agenda) Act 2000 - A New Beginning

Since the Telestra case, Australia has adopted the Copyright Amendment (Digital Agenda) Act 2000. The Act contains a new, far-reaching copyright of "communication
to the public." The Act defines communicate as to "make available online or electronically transmit (whether over a path, or a combination of paths, provided by a material substance or otherwise) a work or other subject-matter." The functions of the broadcasters, cable operators, and ISPs have come under the new right to communicate. The Act has limited the liability of ISPs. In determining whether the ISP authorized the infringement committed by a third party, the court looks at:

1) Whether the ISP had the power to prevent the infringement;
2) The nature of any relationship between the ISP and the infringer; and
3) Whether the ISP took reasonable steps to prevent infringement.

The Act does not hold the ISPs responsible, if an ISP's only role in the transaction is to provide the server by which the infringing material is distributed to the public. This releases ISPs from allegations of authorizing infringement when the ISP is peripherally involved. However, in cases involving direct infringement, the Act states that a communication other than a broadcast is deemed to be made by the person who determines the content of the communication. Since, more often than not, the ISP is not the "person" who determines the content of the communication; the ISP is not liable for infringement.

In contrast to the decision in Telestra, the Australian legislation fully protects ISPs as long as they do not determine the content of the material. Further, in cases where ISPs have to authorize the material, the court looks at the above three elements to determine the ISP's liability.

8.4 The Position in Canada

Canada does not have any specific statutes that deal with the liability of ISPs. The Copyright Act in Canada has two categories of infringement: a) direct infringement, and b) indirect infringement.27

27Copyright Act, R.S.C., ch. C-42 (1985) (Can.).
Direct infringement occurs when any person carries out any act that falls within the exclusive purview of the copyright owner. These exclusive acts include reproduction of a work or any substantial part of the work in any material form, performance of the work in public, communication of the work to the public by telecommunication, or by "authorization" to another person to carry out one of these excluded acts.

In contrast, indirect infringement occurs where a person knows that the work infringes copyright, or would infringe copyright if it had been made in Canada, and

1) sells or lets for hire, or by way of trade exposes or offers for sale or hire;
2) distributes, either for the purposes of trade or to an extent that it prejudicially affects the copyright owner;
3) exhibits the work in public for purposes of trade; or
4) imports the work for sale or for hire into Canada.

Therefore, in indirect infringement, the infringer must have knowledge of the existence of the copyright; while in direct infringement, this knowledge is immaterial. To date, there is no precedent that deals with ISP liability in copyright infringements. However, if the existing provisions of the Copyright Act were to be applied, the results could be interesting.

Anytime that the infringing material is posted on the Internet, any or all the exclusive rights of the copyright holder can be violated. This can draw the ISP into court because the ISP provided the equipment or facilities to a third party that were used to infringe the copyright. Therefore, the ISP indirectly authorized the violation of the exclusive rights. However, in the past, the Canadian courts have determined that merely supplying equipment does not constitute authorization, if the supplier did not retain control over the use of the equipment.28 Moreover, in a recent decision, in de Tervagne v. Beloeil (Town),29 the court clarified that it will not infer any authorization of an illegal act

unless the supplier of the equipment has formed a common purpose with the infringer so as to "sanction, approve, and countenance" the infringement in some way. Applying this principle, most of the infringement that occurs on the Internet arises from users giving commands that result in reproductions or communications of copyright works. These commands are given through the equipment that is provided by ISPs and other intermediaries. ISPs, however, do not have any common purpose with the infringer.

Therefore, it can be concluded that if a defendant took constructive steps to prevent the infringement, or if the defendant had no knowledge of the possibility of an infringement, then the defendant cannot be found to have authorized the infringement. Further, the case law appears to indicate that "authorization" is narrowly construed in Canadian law. It should be noted that the above decisions do not specifically deal with ISPs; rather they provide the courts with guidelines to determine whether an ISP authorized the infringement.

This raises the question of whether an ISP would be liable under indirect infringement. For indirect infringement, an alleged infringer must know that the work at issue infringes a copyright. The plaintiff bears the burden of proving that the defendant had this knowledge. This burden of proof is difficult to carry, because when knowledge is an essential element of an infringement, ignorance can be pleaded as a defense.  

Canadian courts have addressed the term "knowledge" in Section 27(4) of the Copyright Act. The courts construed "knowledge" as a suggestion to a reasonable man that a copyright violation had occurred. Once an individual has either actual or imputed knowledge that the work may violate a copyright, the individual has the responsibility to determine whether the work is infringing. However, knowledge alone is not enough to create liability for a copyright violation. The defendant must also have completed one or more of the actions under Section 27(4) of the Copyright Act. This rule has been substantiated in Apple Computer, Inc. v. Mackintosh Computers Ltd., where an

individual knowingly financed an operation that infringed copyrights, but had not committed any of the actions listed under Section 27(4) of the Copyright Act, and so escaped liability. As for ISPs with knowledge about the infringing activity, they are not at risk for indirect infringement so long as they take steps to prevent the continuation of the infringing activity.

Therefore, in Canada, although there is no current specific legislation, the existing Copyright Act appears to be flexible enough to deal with the challenges of the Internet.

8.5 The Asian Situation - Singapore Leads the Way

Interestingly, some Asian countries like India and Singapore have enacted laws dealing with the challenges posed by the advancements in information technology. In Singapore, the Registry of Trade Marks and Patents formed an Electronic Commerce Committee in 1998 to comprehensively study the issues involved and provide suggestions for dealing with these issues. On August 17, 1999, the Singapore Parliament incorporated these suggestions in a Bill and enacted the Copyright (Amendment) Bill 1999 incorporating it into the Copyright Act.\(^\text{33}\) Under this Act, when the Network Service Provider makes an electronic copy of the copyright material available on the network, it cannot be liable for infringement if:

1) it is made available in the course of providing connections to the copy;
2) the storage, transmission, routing, or provision of connections is done at the direction of a user of the network; and
3) the copy is stored, transmitted, or routed without any deliberate modification of its contents by the Network Service Provider.

However, if the copyright owner provides an ISP with a statutory declaration expressing his belief of the occurrence of a copyright infringement, then it is not exempt from liability for making the material available on the network under Section 193C(1) of

the Copyright (Amendment) Act. This declaration from the copyright owner must outline the reasons underlying the copyright owner's allegations of copyright infringement. The Network Service Provider then has the responsibility of removing the copy from the network or disabling access to the material on the network. If the Network Service Provider fails to do this in a reasonable time, the Network Service Provider is liable.\(^{34}\)

The provisions in the Singapore Copyright (Amendment) Act are similar to the provisions of the Digital Millennium Copyright Act of the United States, where the ISP has to be informed about the violation before liability can attach. In the United States, ISPs must designate an agent with the Copyright Office to allow copyright owners easy access to inform them of violations. In Singapore there is no such requirement, but once an ISP has been alerted by the copyright owner, it has to act expeditiously to remove the infringing material. If the ISP fails to do so, it can be drawn into an expensive law suit. This is an equitable position because it tries to harmonize the interests of ISPs and copyright owners.

8.6 The Indian Position

Currently, in India, ISPs have not been drawn into any major IPR violations. The new Internet policy announced by the Central Government in July 2000 could bring more service providers, in addition to existing ISPs such as Satyam, Dishnet, and Wipro Netcracker. Therefore, in the future, the probability of these ISPs being dragged into unnecessary courtroom battles is high. The law addressing the ISP liability issue is ambiguous. The Information Technology Act exempts ISPs from liability if they can prove that they had no knowledge of the occurrence of the alleged act, and that they had taken sufficient steps to prevent a violation.\(^{35}\)

The Information Technology (Amendment) Act, 2008 brings far reaching changes in Internet Service Provider regime in India. Section 79 of the IT Act, 2000 (as amended) has been substantially amended, expanding the scope of the immunities it seeks to provide.

\(^{34}\)In fact, the new amendment introduces into the Copyright Act 1987 a new 'Part IXA' on 'Works, or Other Subject Matter in Electronic Form', comprised of sections 193A, 193B, 193C, 193D, 193E, 193F, and 193G. \(\^\)

\(^{35}\)See Information Technology Act 2000 S. 79.
8.6.1 Definition of Intermediaries

The amendment provides clarity on the class of intermediaries on which Section 79 is applicable. The concept of network service providers has been done away with (the term “network service providers” in the old Section 79 was by and large redundant, since the explanation to the section provided that the term was to be interpreted to mean intermediaries). The immunities are now available to an intermediary which has been defined under Section 2(w). Section 2(w) has also been amended and now provides an expansive and comprehensive definition of intermediaries. The term intermediary now include telecom service providers, internet service providers, web – hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes. In my opinion, there is no other legislation on the subject which extends immunity from liability to such a wide class of intermediaries. In fact, the extent of immunity available to intermediaries such as search engines, cyber cafes is greatly disputed in many jurisdictions such as the United States and the EU, and has been a subject of judicial deliberation. By providing such a wide definition to the term ‘intermediary’, the availability of immunities to such categories of intermediaries in India is established by the statute itself, thereby leaving no room for judicial vagaries.

8.6.2 Immunity under any law in force

The most significant ramification of the amendment is that the immunity under the IT Act now extends not only to the liabilities arising under the IT Act, 2000 but to liabilities arising under any law in force in India. Therefore, an ISP can claim immunity from liability under Copyright Act, 1957 or criminal liability under the Indian Penal Code by virtue of Section 79 of the IT Act, 2000. This change has been brought about by the introduction of a non – obstante clause in Section 79 which provides that the immunity shall be available to intermediaries ‘notwithstanding anything contained in other law for the time being in force’.

8.6.2.1 Scope of the immunity available to intermediaries

Section 79(1) of the amended Act stipulates that intermediaries shall not be liable for any third party information, data, or communication link made available or hosted by him. The plain reading of the Section indicates that the scope of the liability is very wide,
and is available for any third party content hosted by the intermediary. Thus, the
immunity under Section 79 is available to the intermediary irrespective of whether such a
content is copyright infringing or defamatory or obscene in nature.

8.6.2.2 Exceptions and conditions

That being said, it is pertinent to note that Section 79 does not provide blanket
immunity to intermediaries. Section 79(1) is made subject to the provisions of
subsections (2) and (3) of Section 79. Section 79(2) stipulates certain conditions required
to be fulfilled by intermediaries for claiming the immunity. Section 79(2) contains 2
disjunctive conditions under clause (a) and (b). Clause (a) protects 'access only ISPs' i.e.
those intermediaries whose role is limited to providing access to a communication
system. Clause (b) has been borrowed from Regulation 17 of the Electronic Commerce
(EC Directive) Regulations, 2002 and in essence provides that the intermediary must not
exercise any 'control' over the information for claiming immunity. Therefore to claim
immunity, the immunity must not be involved in the initiation of transmission, the
selection of the receiver of such transmission or the selection or modification of the
information. Involvement in any of these three acts would make the immunity
unavailable to the intermediary.

Further, in addition to above two disjunctive conditions, the intermediary is
required to exercise due diligence for claiming said immunity. Now, the standard of due
diligence which the intermediaries are required to exercise shall be subject to judicial
interpretation. In my opinion, this shall form a major bone of contention in most ISP
liability cases, since due diligence is a vague and nebulous concept, and its exercise or
lack of is a debatable issue. The case of Avinash Bajaj v. State of Delhi36 (the famous
Bazee.com case) provides some guidance as to the level of due diligence expected from
ISPs. In this case, the Court held that the ISP had failed to exercised due diligence. It
based its finding on the fact that the website failed to provide for efficient filters to screen
pornographic content and it failed to introduce any operative or policy changes to prevent
the listing/display/sale of the same on the portal. Section 79(3) provides for cases where

---

36[150 (2008) DLT 279]
the intermediary in which disentitled to claim the immunity. As per Section 79(3)(a), the intermediary is not entitled to immunity where it aids, abets or induces the commission of the unlawful act. This is to impose liability in cases where the intermediary is activity involved in the infringing activity.

Secondly, the intermediary is required to remove the infringing material on receipt of notice of the same. It is pertinent to note here that there are no counter notification procedures under Section 79. Such counter notification procedures are essential to ensure that services of the intermediary is not jeopardized by frivolous claims by right holders. The DMCA, 1998 which provides for such counter notification procedures mandates the service provider to restore access to the information at the direction of the alleged infringer who feels that he or she has been wronged by such removal. Without such counter notification procedures, Section 79(3) (b) of the IT Act, 2000 (as amended) has immense potential for abuse, and can be misused by right holders even in cases where no bona fide claim exists.

8.6.3 Liability to be imposed under other Acts

It bears noting that where the conditions under Section 79(2) are not satisfied or where the exceptions to liability are applicable, the liabilities can be imposed on intermediaries. However, Section 79 of the IT Act only contains the immunities available to the intermediaries. Thus where liability is to be imposed on intermediaries, it can be done only by reference to other statutes such as the Copyright Act, 1957. In my opinion, there is a need for further amendment in these liability – imposing statutes, since the traditional provisions contained in these statutes are insufficient to effectively deal with complex issues of intermediary liability.

Lastly, the amendment to Section 79 of the ITAA, 2008 is a laudable effort, since it provides much needed clarity regarding the immunities which are available to intermediaries under Indian law. The conditions and exceptions provided under Section 79 are by and large able to strike the right balance between the interests of the right holders and the ISPs. However, further amendment is required for introduction of counter notification procedures as well as in liability – imposing statutes in order to establish a
comprehensive and exhaustive statutory mechanism for dealing with issues relating to ISP liability

8.7 Conclusion

After reviewing some of the "cyberspace" legislation, it is not surprising to find that the legislation in this field lacks clarity. The Digital Millennium Copyright Act of the United States has clearly defined the standard of knowledge an ISP is required to possess for it to be held liable for illegal third party activities. The Digital Millennium Copyright Act allows ISPs to terminate the accounts of individuals who infringe copyrights on a regular basis. Furthermore, in the United States, ISPs have to register an agent with the appropriate office so they can receive information of copyright infringements. This eliminates the possibility of an ISP being caught unaware of third party infringements.

As is seen, the EU Directive has some loopholes that need to be closed. The most troublesome of which include, a lack of a "notice and takedown" procedure, which threatens freedom of expression; and the fact that the current regime may actually promote unfair competition in some situations. The lack of a notice and take down procedure causes the ISPs to become a sort of censorship body, in order to avoid liability when they opt to take down a Web page upon receipt of a claim regarding the content on that page. This threatens freedom of expression as long as customers are without protection against unfounded complaints. Unfair competition may be promoted in cases where companies engage in a form of commercial war in cyberspace, lobbing bad faith claims against their competitor's Web content.

A notice and take down procedure modeled after the DMCA be established, including notice to specialized bodies within the Member States' administrative structures or professional organizations. Regarding the second Achilles heel of the EU Directive, in order to have a complete protection for all the parties involved, a "put back procedure" should be initiated. Such a procedure should give the owners of disabled Web sites the chance to exercise a defense and at least stave off an unwarranted blocking or removal of their content. Finally, liability must be imposed upon persons who intentionally transmit false or unfounded notices which lead to the removal of a Web page content.