CHAPTER 8

CONCLUSIONS AND SUGGESTIONS
CHAPTER 8

CONCLUSIONS AND SUGGESTIONS

Technology is copyright’s best friend and worst enemy. The copyright industry is at crossroads once again in the global digital economy and faces yet again a challenge which is unprecedented in magnitude and consequence. This junction is, in many ways, a defining moment in the long and chequered history of copyright. The people out there have gone to the extent of declaring and announcing, ‘copyright is dead’. But the concept of copyright lives on in the statute book and will continue to stay there as long as the concept of property remains valid in human society because in the end copyright is just an extension of the concept of property to the intellectual domain. This approach of thine and mine will necessitate the continuation of the copyright application in the cyberspace. Therefore, it is not the future existence of copyright but rather the future design of copyright that should be a matter of concern.

Intellectual property laws are based on notions of sovereignty and territoriality. The Internet, in contrast, like the movement of weather within the global climate,
largely ignores distinctions based on territorial borders. The Internet, the world’s biggest copy machine, has been described as the greatest threat to copyright. The free flow of information that is the very culture and value of the Internet conflicts with this copyright interests. Never before has it been so easy to violate a copyright owner’s exclusive right to copy the material. The intellectual property discipline is confronted with new issues generated by the emergence of the Internet. Each of them must successfully resolve these issues in order for electronic commerce to flourish. It is therefore important to adjust the legal system to respond to the new technological environment in an effective and appropriate way, and to do so quickly, because technologies and markets are evolving rapidly. Accordingly, the goal of policy makers has been to achieve an appropriate balance in the law, providing strong and effective rights, but within reasonable limits and with fair exceptions. In our quest to find a proper balance and seek the future design of the copyright law we have arrived at the following conclusions and suggestions.

The Web sites are soaked in information, much of it with varying degrees of copyright protection. In fact, the reality is that almost everything on the Net is protected by copyright law. Since, designing, producing, and maintaining a sophisticated Web site is very expensive, protecting content ownership is extremely important. Never before has it been so easy to violate a copyright owner’s exclusive right to copy the material. Contents of a Web site can be exploited by another Web site by the practices of linking, inlining and framing technologies. The interactive feature of the Internet’s most popular information access tool, the World Wide Web, to hyperlink\(^1\) defines its very culture distinguishing it from any other communications medium. What liability is there for the content on a linked site? A site employing the practice of deep linking could be held liable for unauthorised distribution of copyrighted content belonging to another site. So, should the law be amended to stop deep linking without permission of the owner of the content? Or should the law provide complete

\(^1\) On the Web or other hypertext systems, hyperlink is a synonym for both link and hypertext link.
immunity to links of all kinds. Internationally, no law till date has put a ban on deep linking. There are indeed problems in doing so. On the one hand one has to consider the rights of the owner of content and on the other hand the interests of the society for which growth of the Internet is all important. The international treaties and laws do emphasise the importance of control in the hands of the content owner, but specifically they have not dealt with the problem of deep linking. It would not be proper for the Indian legislation to include a provision banishing deep links altogether because the current provisions\(^2\) are sufficient to check the unauthorised use of someone's content through deep linking and using these provisions courts can fill the vacuum by deciding from case to case basis; if a deep link has been created with bad intent and in order to derive unjust enrichment out of somebody's content then it could be injunctioned.

Imagine a situation akin to the *Washington Post*\(^3\) case. The world renowned news portals make huge investments in terms of time, effort and cost to bring a news report. What if someone just frames the same by a simple technique? It would be wholly unfair to do so or to allow so. Should the law, then be amended to outlaw inlining and framing or to allow these practices? The practice of inlining and framing could implicate the distribution, communication, adaptation and moral rights in case of copyrighted content. The Copyright Act talks about various rights of owners and authors of works and describes situations where these rights can be infringed. The provisions\(^4\) of the Copyright Act, 1957 are sufficient to tackle the situation of unauthorized use through inlining and framing. In this situation and there is no need for any amendments in this regard. It is for the courts to decide upon the legality/illegality of framing from case to case. The measure would always be the Copyright Act, the philosophy of which is amply clear. In case an inline image or a frame amounts to aiding in distribution or

\(^2\) Ss. 2(ff) read with s.14 and s. 51 of the Copyright Act, 1957.

\(^3\) 97 Civ.1190 (S.D.N.Y.).

\(^4\) Ss. 2(a), 2(ff), 14, 51 and 57 of Copyright Act, 1957.
communication with dishonest intentions, the courts will come forward and declare such infringement illegal.

Multimedia works on the Internet have caused some concern for the rightholders. The user can 'interact' with a multimedia work in ways previously unknown. He can make alterations and additions and even create a new work out of the stock of existing ones. If the rights for all classes of works were the same, then perhaps, this would not have been a major issue. But the law as it stands in India, distinguishes between different classes of works in the matter of rights. The authorship may raise another problem, as the criterion of authorship is different between literary, dramatic, musical and artistic works on the one hand and cinematographic films and sound recordings on the other hand\(^5\). What kind of protection does a multimedia work attract in its individual combination of component parts. The significance of the issue lies in the fact that the relevant categorization entails different legal consequences and the presence of multimedia work defies existing classification under the copyright law. It is not a new type of work to the extent that a multimedia product can fall under one or several, already existing, categories. Protection of the individual elements of a multimedia work must not be confused with protection of the multimedia production as a whole. In accordance with the existing provisions of the Copyright Act it remains possible to dispose of the individual contributions separately, even after the individual elements have been combined in one single work. The actual classification of a particular multimedia product will depend on the type of work and on the different and specific characteristics of each individual multimedia product. Therefore, it has to be decided on a case-by-case basis. To the extent it is a literary work it gets protected as such; to the extent it is a cinematographic work, it attracts copyright protection as a cinematographic work and to the extent that it is a pure phonogram, its producer is protected. The final interpretation, of course, will then often be in the hands of the courts. But under which category can one register a multimedia work? The fact is that a

\(^5\) S. 2(d) of Copyright Act, 1957.
multimedia work taken as one single product does not exactly fit any of the existing categories of works protected under the regime of copyright. But, it is possible to consider and treat multimedia products as works similar to cinematographic film in the sense of section 2(f) of the Copyright Act, 1957. It seems possible to classify and to treat multimedia productions as collections of literary or artistic works in the sense of Article 2(5) of the Berne Convention and they might also fall under the category of compilations of data or other material in the sense of Article 10(2) of the TRIPS Agreement. There is also a view that multimedia work, being a digital product, be classified as computer programme. Since there are separate provisions for rights and authorship of a computer programme as distinct from literary works in the Copyright Act, this could be a possible solution. However, issues may arise on the retention of separate copyrights in the works incorporated in the multimedia, in terms of section 13 of the Act\(^6\) and the rights of performers\(^7\) in the product. At present, large numbers of multimedia works are being created by combining pre-existing works. The classification of multimedia works is an issue, which needs to be looked into in depth. It still remains to be decided whether multimedia works should be regarded as a separate category of works protected under the regime of copyright. Since it has not yet been clarified to what extent multimedia works fall within one of the above-mentioned types of work, it should be pointed out in legislation that a work can consist of the combination or merging of other works. This would ensure that the prerequisites of protection were not examined separately but in relation to the multimedia work as a whole, which would enable protection of the interactivity so characteristic of many multimedia works, provided that it fulfils the originality requirement. So, the Copyright Act should be

\(^6\) S. 13(4) of Copyright Act, 1957 provides:

The copyright in a cinematograph film or a sound recording shall not affect the separate copyright in any work in respect of which or a substantial part of which, the film, or as the case may be, the sound recording is made.

\(^7\) As per s. 38(4) of Copyright Act, 1957 once a performer has consented to the incorporation of his performance in a cinematograph film, his performer’s right in that performance ceases to exist, whereas in the case of other classes of works there is no such provision.
amended to include multimedia work as a separate category which is recognised, protected and can be registered as such.

As traditional broadcasting has developed a number of other services, a number of new players have become involved in the transmission of both traditional broadcasts and, in particular, of new types of services and programs. In terms of size and character the traditional and new are very different, spanning from large national broadcasting corporations operating under well-defined rules to private individuals operating in the absence of rules. The Internet has become another way of broadcasting copyright protected content, for example through webcasting which is the real-time transmission to the public in a digital format of audio and audiovisual works. Webcasting over the Internet is similar to broadcasting but uses special technology to reduce the size of the digital files being sent. Webcasts are widely available to anyone with a computer connected to the Internet. The world of broadcasting, as we have known it, is about to change with the leading broadcasting organisations ready to jump on the Internet bandwagon. Webcasting has a promise of presenting content which fits the slogan of ‘anything, anytime, anywhere’. Webcasting opens new opportunities for authors and performers to expose and market their works to new audiences, and for the public to enrich their understanding and appreciation of cultures from around the world. Rather than creating a homogenization of experience, webcasting emphasizes the importance of local culture. An Internet channel from India, Nigeria, USA or Australia, for example, will attract listeners from around the world primarily because it provides a window to local information, news, customs and arts. In view of the growing importance and widening reach of webcasting and increasing incidents of piracy involving webcasting, it has become extremely important for national laws and international conventions to address this phenomenon which till now has been ignored.

Broadcasting organizations have in the past been granted protection for the result of their investment, their entrepreneurial efforts and their contribution to the...
diffusion of culture and their public information service. The same interests that initially impelled protection of copyright and neighboring rights for broadcasting now compel adoption of equivalent protections for webcasting. Webcasters create and transmit valuable content reflecting creativity and authorship, as do traditional broadcast media. Copyright and neighboring rights protection should be made available to such works, and protection should not be denied merely on the basis of technical methods of delivering such works to the public. Even for works consisting of retransmissions of terrestrial radio or television broadcasts, it would be illogical and irrational not to offer protection, as piracy over the Internet is more widespread and commonplace. But what should be the mechanism of protection? Should webcasts and webcasters be protected independent of broadcasting? Or should webcasting be assimilated to broadcasting in terms of protection? In view of convergence of various technologies and services, and considering the threat of piracy both by webcasts and of webcasts, in our opinion, it is only appropriate to assimilate new activities of webcasting to traditional broadcasting.

To protect Internet webcasting, the definition of “broadcasting” in the Copyright Act should be updated in two ways. First, the definition should encompass ancillary data that may be included in the transmission. As noted above, Internet transmitting organizations may send related and ancillary text, graphics and images along with the audio or audiovisual works. Such data may include, for example, information concerning the works being performed; information concerning the performers; links to the Web sites of online retail establishments from which the listener or viewer can purchase the particular phonogram or audiovisual work being broadcast, or tickets to concert performances, etc. As a whole, this capacity results in rich and creative forms of broadcasting content which merit full protection. In this respect we note that even traditional broadcast media also have been embedding data into their signals, such that suitably-equipped receiving devices may display data such as the name of the broadcast station, weather, traffic, sports scores, stock information, and so forth. The
definition of "Broadcasting" should include all transmission modes and associated text and data. We, therefore, propose that the definition should read:

"broadcast" means communication to the public--

i. by any means of wireless diffusion, whether in any one or more of the forms of signs, sounds or visual images or any related or ancillary data or text transmitted by the transmitting organization; or

ii. by wire; and includes a re-broadcast;

Second, the expressions used in international treaties is “public reception” and the expression used in the Copyright Act, 1957 is “communication to public”, which seem to imply that only the process of ‘point-to-multi-point’ is covered under the definition of broadcasting leaving the process of ‘point-to-point’ transmission in case of webcasting. Therefore, the concept of “communication to public” in the Copyright Act, 1957 should be understood to include the making available of transmissions whether by broad diffusion of signals or ‘point-to-point’ transmission.

The subject of protection, is the broadcasting organization. Which type of organizations is protected as broadcasting organizations under the Copyright Act, 1957 or the 1961 Rome Convention is not expressly clarified. Although there is no definition in either of the instruments of “broadcasting organization,” it was and is generally accepted that these are organizations which provide their broadcasting services to the general public over Hertzian (wireless) waves and wires. In this respect, following technological developments new program transmitting entities have emerged, and the question has been raised whether every entity distributing signals and involved in the distribution of programs would qualify as a broadcasting organization and benefit from the protection. With the arrival of the Internet it has become comparatively easy and within the reach of individuals to engage in lawful and unlawful activities of webcasting. Practically,
it would take little time to set up an Internet radio station, which on the off-line media would be a Herculean task and was typically restricted only to organisations. Therefore, in legal instruments we find that the subject of protection is invariably ‘broadcasting organisations’. In this light it becomes necessary to define afresh the subject of protection for broadcasting activities.

The Rome Convention states that the term of protection shall last at least until the end of a period of twenty years computed from the end of the year in which the broadcast took place. Whereas section 37 of the Copyright Act, 1957 states the term to be twenty five years. In this regard, there is no need to take any position on the appropriate term of protection for webcasts; just the term of protection for webcasts should be coextensive with the term of protection for other broadcasts.

Peer-to-peer (P2P) has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server. Recently, P2P networks such as Napster, Gnutella and Kazaa have led to massive reproduction and distribution of copyrighted works on a scale which is of unprecedented magnitude. To stop this rampant piracy the copyright industry has fought the war against such P2P networks and their users with lobbying, litigation, copy protection technologies and self help measures. The audiovisual industry could entrap the first of such P2P networks namely, Napster and similar services with the help of copyright law. Napster, though dead, but has been the progenitor of numerous similar applications like Gnutella and Kazaa. There have been vigorous legal battles between the audiovisual industry and these services but, because of their inherent architecture, nothing could be done against them. Gnutella and Kazaa are legal; there is no law against sharing public domain files, meaning thereby anybody is free to use Gnutella or Kazaa for sharing content that is in public domain. It's when people use Gnutella to distribute copyrighted music and films that its use becomes illegal. The content industry is officially upset about Gnutella and Kazaa, but there is currently no easy way to control it.
If any person is running a network like Napster in India he could be liable for encroaching upon the exclusive rights of the copyrights owner as he is essentially facilitating the communication of the work to the public. As for the persons who actually make available and download copyrighted works, the law is very clear. Section 14 of the Copyright Act, 1957 says that issuing copies of work or communicating the same to public amounts to infringement. So, a person who downloads a software like Napster and implements the same on his machine is making the copyrighted work available to any member of the public who has the corresponding software installed on his machine. The person who actually downloads the file containing copyrighted work is reproducing the work without the consent of the copyright owner, so is guilty of copyright violation as well. Section 51(b)(ii) of the Copyright Act says anyone who distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright. Any person making available copyrighted works over P2P network may not be trading in the same but he is nevertheless distributing such work which combined amount to gigantic proportions affecting prejudicially the interests of copyright owner.

Now for networks akin to Gnutella or Kazaa, where there is no central server brokering the requests of people, it is rather hard to stop the system in one go. There is no one person or entity that is managing the affairs. The entire thing is managed by a software and that is already out and lakhs of people have made copies of the same. You can't really outlaw the installation and use of that software as it could legally be used for sharing files which are not protected by copyright. But individuals who use such software for sharing copyrighted works remain guilty under the above stated provisions of Copyright Act.

The Recording Industry Association of America (RIAA) blames 5.3 and 7 percent drops in the number of CDs sold in 2001 and 2002, respectively, in part on online

---

8 S. 14 read with s. 51 of the Copyright Act, 1957.
file trading. According to the RIAA, the decline cost the industry $284 million in lost sales. According to The International Federation of the Phonographic Industry, IFPI, for the year 2001, worldwide record sales were US$33.7 billion dollars. The availability of free music on the Internet was blamed for the 5% drop in global sales of compact discs. In the year 2002, global sales are down 9.2%.

World sales of recorded music fell by 10.9% in value and by 10.7% in units in the first half of 2003. The stakes are high all around. The Industry points the finger directly at the Internet. But these figures have all been brought out by the Industry. Moreover, it can't be said with unfailing certainty that how much of this loss is due to online piracy. So, on the question of the impact this activity is having on entertainment company profits, we remain agnostic: other factors, such as the state of the economy, and the easy availability of content on alternative media like television channels will also have a bearing on the sales of pre-recorded music, films and software. There is also a tendency by the entertainment industries to argue that every copy made through the medium of file-sharing is a lost sale. That begs the question as to whether the person who made the copy would have actually paid to acquire a legitimate copy had the alternative not been available. In India, the problem of infringement through the Internet has yet to reach the magnitude that it has in some developed countries—we have had no Napster-like problem on anything like the same scale, audio cassettes still being the most common and most accessible form in which copies of sound recordings are stored, being much cheaper and more widespread than the digital alternatives. That situation could no doubt change.

The online file-sharing service demonstrated that people using readily available equipment could easily download and distribute digital music and movies en masse, regardless of copyright. Not surprisingly, that sent the copyright industry, particularly the audiovisual industry into a panic. Shocked and dismayed, the

9 IFPI comprises a membership of more than 1500 record companies, including independents and majors, in over 70 countries (http://www.ifpi.org/).
industry in the last couple of years has been fighting this menace of ‘piracy’ on all possible fronts, that include, lobbying, litigation, legislation and technological measures.

Not getting their way, the industry is starting to move down the food chain, prosecuting not only companies like Napster but also individuals who download copyrighted content. That sets us to find why do people do what they do? An important question in this respect is why ordinary people who are generally speaking law-abiding citizens engage in the online use of music and films that according to national and international law is unauthorized. The answers to this could be many. One, people do not consider this use unauthorized. Ordinary people in their role of consumers tend to regard digital content as something that is out there in order to be shared by all. This is particularly so with popular music which is not perceived as the product of a creative music industry which has to invest vast sums in its promotion and distribution, but rather as a freely circulating part of culture.\footnote{Willem Grosheide, “The Missing Link: Repairing the Chain From Industry to Customer – The Online Use of Music and Text”, paper presented at ATRIP Congress 2003 at Tokyo, Japan.} Two, until very recently and despite the availability of appropriate technology, the audiovisual industry has failed to offer its customers the products they want. If under those circumstances the preferred product is available for free on the Internet, it should come as no surprise that people serve themselves.\footnote{Ibid.} Three, this is more so since the production and sale of music has over the last two decades concentrated in a few multimedia giants, which almost completely dominate the supply of music content. In view of how these giants like to present themselves in today’s society, they should not be surprised when people do not seem to feel they are causing any substantial harm to the content industries or the artists and performers they represent.

Consumers for their part have, for obvious reasons, so far hardly been able to articulate and express their views on the social and legal questions with regard to

\footnote{Willem Grosheide, “The Missing Link: Repairing the Chain From Industry to Customer – The Online Use of Music and Text”, paper presented at ATRIP Congress 2003 at Tokyo, Japan.}
the online distribution of audiovisual products, other than by their actual conduct.13 But in this environment is it proper to view consumers as pirates? The industry harps on the doctrine of functional equivalence which means whatever laws apply in the offline world should also apply in the online environment. If somebody goes to a store and steals a CD, he would be prosecuted and made liable for the theft. On a P2P network, without leaving his house, a person could steal material worth thousands of CDs. Should there be a difference? It seems inappropriate to incriminate consumers for piracy when they are file-sharing music or circumventing technological measures to get access to text. This seems inappropriate, because however unlawful such unauthorized file-sharing or circumvention may be under the circumstances, it is not an act of piracy in the proper sense of the word, which would require the organized, systematic infringement of copyright law for commercial purposes by wholesale copying and reselling of illegitimate products. Widespread action against consumers will no doubt put the industry’s relationship with the public under further strain.

The communication of online audiovisual products is in great disarray, as is evidenced by an ongoing societal and legal process of action and reaction between the established music industry, suppliers of file-sharing software, Internet service providers and individual users. In an environment where the audiovisual industry has put itself in conflict with its own consumers and other industries like that of technology producers and ISPs, questions are being raised about the legitimacy of copyright system in the digital landscape. The issue of the legitimacy of copyright law as a system of positive law may be looked at quite differently depending on whether it is approached from the perspective of a country with an established and expansive audiovisual industry or from that of a country which depends on the import of foreign materials for its public. A country having large audiovisual, music and film industries will tend to regard copyright system in high regard and a country not having large industries of their own will

13 Ibid.
do otherwise. It depends on which side you take. Seen in this context, the legitimacy issue touches upon the question of North-South relations. Even in the Western world where arguments in favour of copyright and other IPRs are vociferous the legitimacy of copyright law is being questioned, as is illustrated by the fact that the RIAA is allegedly preparing legal action against millions of individual users of music file-sharing software.¹⁴

P2P file trading is a global phenomenon. Although record companies have won considerable victories with the enactments like the Digital Millennium Copyright Act (DMCA), Napster’s bankruptcy, and tools enabling the encryption protection of CDs to prevent copying, they have progressively lost a substantial consumer base. Stronger and more uncontrollable P2P networks have emerged since the death of Napster, hackers have easily circumscribed copy protection technology, and consumers are fighting for the fair use rights. The continued growth and popularity of P2P networks is not likely to cease in the near future. It’s hard to get the genie back in the bottle. The record industry has fought the war against music piracy with lobbying, litigation, copy protection technologies and self help measures. The industry cannot possibly win a war fought on all fronts has to think in terms of change its business model. Entrepreneurs will have to think about change in business models and reducing prices so as to be viable to the digital market. Public education and awareness about copyright is also important. Consumers will have to learn and be comfortable shopping at their computer than in stores, and until that community feels comfortable about the security of their financial transactions, the market is going to be 99% hype and 1% wish. All sides should come together and work on a way to pay the royalties and embrace the current technology. The digital product industry, artists, ISP’s, software firms, computer manufactures, blank CD makers, and P2P networks need to find a middle ground and a way to pay royalties to their rightful owners.

As more and more digital products in network environment are emerging, efficient management and controlled distribution of such products has become one of the important considerations, as never before. The primary requirement for the automated grant of rights in a digital context is that the protected work and subject matter can be identified as such belonging to the relevant authors and rightholders and the licensing terms must also be available electronically. Rights management information which identifies the work, the author of the work, the owner of the work, or provides information about the terms and conditions of use of the work which are necessary for licensing and payment of licence fee, are essential in the digital networked environment and must be protected by law. Rights management information in the digital age has become the bedrock on which author of a work could claim his economic and moral rights because in the digital age it has become very easy and within the reach of ordinary people to detach the author's name from the work and put someone else's name in its place; manipulate with a work so as to distort or mutilate the same. Therefore, legal recognition and protection to rights management information have been provided in WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) and have come up in a number of national legislations which penalise anybody tampering with such rights management information employed. In this direction suitable amendments should be made in the Indian Copyright Act barring any manipulation with rights management information on lines of the WCT and WPPT which will help rightowners exploit their intellectual property on the Internet.

When a digital product is made available for access on the Internet, anyone in the world becomes capable to download the product free of charge, use it without restrictions, incorporate the product into his own product and make the resulting product available in a global network, hence competing with the product of the creator himself. In order to fight this loss of control over the product in the digital environment the legal instruments as such are not sufficient. To a large extent the solution to a loss in technical control should be sought in technology itself.
Increasingly, technological solutions are being found for the problems posed by the new technologies through access control or copy control mechanisms such as encryption technology or water marking incorporated into works distributed over digital networks with a view to protecting them from illegal exploitations. The debating point here is that should we make it compulsory for hardware manufacturers and software producers to employ copy control mechanisms? The situation in which India finds itself today, we should not hastily move towards making it compulsory for technology makers to implement certain copy protection standards. India has low information technology product penetration and in rural areas it is all the more limited. The computer hardware industry is fledgling and should not be asked to comply with new standards of copy protection. In case we do the same, it will not only force the hardware industry to increase prices for additional implements, it will also force consumers to pay more. Moreover, there could be compatibility problems between new and old machines. So, restraint is better than rushing as far as the implementation of copy protection technology is concerned.

Apart from managing intellectual property through technological measures and accompanying legal provisions the copyright industry is also employing considerable self-help countermeasures since other efforts to thwart piracy on the Internet are not working to give desired results. Most of these self-help measures like 'file spoofing' and 'swamping the search' would be termed illegal when tested on the touch stone of laws like the Information Technology Act, 2000. Spoofing, swamping or any other measures adopted on the Internet may also lead to unwanted damage to computers, networks or servers belonging to persons who may have played no role in alleged copyright infringement. In the light of this it is not wise to adopt self-help measures in managing intellectual property on the Internet. Since validating self-help measures would amount to giving ordinary individuals the authority to take law in their own hands, any move
to validate any of the self-help measures should not be encouraged in India as is being done in the USA.\textsuperscript{15}

The copyright limitations are inserted within the copyright legislations to ensure that the deadweight loss caused by the exclusion of non-rival uses does not outweigh the gain in social welfare which follows from the incentive to create. There have always been a number of limitations and exceptions which evolved, not only to give the author sufficient incentive to produce new works to satisfy the public interest, but also to ensure that parts of existing creative works are available to build upon in the creation of new works. Unfortunately, copy control technology doesn't affect only pirated distribution on the Internet networks--it can prevent users from making any copies at all, even ones that formerly would have qualified as fair use. In the context of limitations on copyright, evolutive amendments to the existing limitations are advisable. The amendments are to be guided by the principle that the exclusive rights should be limited to the smallest possible extent and to the extent necessary in order to arrive at a reasonable balance between the interests of all participants in the digital environment. Consequently, the current wording of the existing provisions should be examined from the following perspectives:

- it should be broadened where it is too narrow to fulfill the previous purpose of the relevant limitation, in a digital context;

\textsuperscript{15} There is a move to adopt new laws that would validate self-help measures. But there are great dangers in that. On July 25, 2002, a bill was introduced in the House of Representatives of the USA that allows copyright owners to "be able to use reasonable, limited self-help measures" to stop the unauthorized sharing of their copyrighted materials on P2P networks. The bill is designed to enable copyright owners to fight individuals trading copyrighted files through the P2P networks. This bill will allow hacking into computers to look for copyrighted information, blocking of file transfers, and adding fake files into the information stream to fool downloaders. Copyright owners would be provided a safe harbour in which they could disable, interfere with, block, divert or otherwise impair trading through a peer-to-peer network without criminal or civil liability.
• it should be narrowed where it embraces digital exploitation but where the interests of rights holders would thus be impaired unreasonably;
• in view of the specific nature of digital exploitation of works, the extent to which additional exceptions should be laid down to the benefit of users should be examined.

It should be clarified that digital reproduction, i.e. making of a single digital copy of a work for private use and for personal scientific use, as well as inclusion of a work in digital archives for private and personal scientific purposes is permissible without the author's consent, provided that a personal copy of the work is used as the model for the reproduction. Only personal making of copies, not making by another person should be permissible.

In the digital medium, the doctrine of fair use is also being watered down by a combination of legislative provisions and contractual terms. This enables the hi-tech companies to curtail the freedom of users to deal with the digital products by means of imposing legally binding contractual terms which extend to the gagging of fair use in digital products thus extending the reach of copyright protection far beyond the scope envisaged under the legislative provisions. Since fair use provisions are designed keeping in mind the public interest and in order to foster future creativity, modifications in fair use provisions by contracts should not be permissible.

Along with the invention of technical measures for protecting copyright works in the digital networked environment, counter-technologies are developed to defeat those protection technologies making it possible to circumvent each and every technical protection measure by using technical means. Circumventing an effective copy control might be regulated as a preparatory act for copyright infringement or a kind of “indirect, contributory” wrongdoing. Should the law then penalize manufacture of the hacking device or end user’s circumvention? Legislating in this area is fraught with danger as potential chilling effect resulting
from a regulation banning every circumvention need be considered too. Employing copy protection may become necessary for copyright holders in the digital age; otherwise everybody would be free to use the digital product without paying for the same. But this copy protection can also lead to further restrict the fair use of a copyrighted work, thereby affecting the public interest implicit in the concept of copyright. The intersection between technological protection measures and limitations on copyright is undeniably the thorniest issue confronting lawmakers around the world in the field today and there is reason to fear that the exercise of legitimate limitations on copyright may be seriously compromised in the digital networked environment through the application of technological protection measures. Technological protection measures allow the exclusion of uses. However, while copyright is limited in many ways (by its term, its object, the scope of the restricted acts and the explicit statutory exemptions), exclusivity based on technology is potentially unlimited. It may, for example, be possible by way of technology to exclude others from using information which is not copyrightable, or to exclude acts which are not restricted acts under copyright, either because they do not fall under the definitions of the exclusive rights or because they are explicitly exempted.16 How should the legislator then deal with this phenomenon of expanding exclusion? Should he maintain the information policy which is expressed in copyright law - of which the limitations on the right are an integral part - or should he endorse the broader exclusivity based on technology? Do the changing circumstances in the on-line environment perhaps require more or less exclusivity? Assuming that copyright law reflects some sort of balancing process, it is too early to know whether - to even the scales again more weight should be attached to the copyright holders' interests or rather to the interests of information users. Moreover, the technologies which will be used for circumvention of technological protection measures will also have

many other uses different from inducing copyright infringement. In this situation, including an anti circumvention provision in the Copyright Act will only be an exercise in futility. Thus, for now no such provision is needed in the Indian statute on Copyright.

Because of the inherent difficulties of enforcing copyrights against individual Internet users worldwide, the copyright owners have found the answer to this problem in placing legal liability for intellectual property infringement on those who allow and enable Internet pirates to exist, namely the Internet service providers (ISPs). Most of the time in every set of action that a copyright owner takes against infringements on the Internet, by and large the action is simultaneously taken against the ISP as well, apart from the person who actually commits the infringement. There are reasons behind ISPs being sued so often when it comes to Internet infringements; and this is true not only for copyright infringements but also for all other kinds of infringements that take place on the Internet. The reasons are that it is easier to trace ISPs rather than individual infringers; it deters infringement by others; and ISPs as business entities have deeper pockets to pay damages. The issue of on-line copyright infringement liability for ISPs has been around since the use of the Internet started to expand rapidly in the early 1990's and has been the subject of extensive debates worldwide. Should ISPs be held responsible for illegal activities committed by their users? Should on-line intermediaries be held responsible for third party material put on the Internet by users of their facilities? If yes, what should be the extent of their liability?

ISPs are the prime movers of ‘information’ which is the raw material in knowledge economy. It was truly said for the last millennium that ‘a man without roads is a man without civilisation’. For this millennium we can verily say that ‘a man without information is a man without progress’. In a world where the growth of ISP industry is directly proportional to the spread of information and connectivity is used synonymously with advancement, the ISPs as transporters of the
The liability of ISPs may arise in a variety of legal fields, such as criminal law, tort law, trade secret law, copyright law, trademark law, unfair competition law, etc. In the quest for a sound regulatory framework governing the activities of the ISPs worldwide many nations have tried to define the liability of ISPs in disseminating third party content. Many of these national laws relate to criminal law, information technology law or copyright law. These statutes have tried to solve the problem by adopting either of the two approaches; horizontal approach and non-horizontal approach. The horizontal approach covers not only copyright infringement but also all other potential areas of law where liability of ISPs might arise. It fixes the liability regardless of the grounds for illegality of the transmitted material. Whereas, under non-horizontal approach the potential liability of ISPs is determined under each law where it might arise. In this case various statutes would determine ISP liability; for example, adopting non-horizontal approach the copyright statute would address ISP liability that might arise only in relation to copyright violations. The Copyright Act, 1957 was obviously drafted in complete oblivion of the phenomenon called the Internet. Even after its amendments in 1994 and 1999 it does not contain any express provision for determining or limiting ISP liability. However, some provisions in the Act could be interpreted to have some bearing on the liability of ISPs. As per section 51 (a)(ii) and section 63 of the Copyright Act, ISPs can be made secondarily liable if they knowingly allow their facilities to be used for copyright violations.

The preponderance of legislations around the world containing limitation clauses for ISP liability make us safely conclude that their liability has to be limited. The IT Act, 2000, which follows a horizontal approach, is a welcome step towards this direction but it needs to be amended on many a count. Keeping in mind the situations and characteristics of Indian legal system, it is only wise to have adopted a horizontal approach for determining the liability of ISPs, i.e. their
liability should be defined as per the existing statutes for contributing to illegal
activities and then it be filtered through the IT Act. In this regard the Copyright
Act need not be amended and the existing provisions can be used to determine
the liability of ISPs. The same is true about all other laws where the liability of
ISPs might arise.

In India the provisions relating to the ISPs are specifically legislated in the
Information Technology Act, 2000 where an Internet Service Provider is referred
to as Network service provider. The concept of ISP is quite wide and subsumes
within itself many roles within the domain of network communications. World over
various statutes dealing with the liability of ISPs have classified ISPs into
different heads like access providers, hosting service providers, etc. and their
liability depends on their respective role in overall network communication.

Under IT Act, 2000 no classification of ISP has been attempted. The expression
‘Network service providers’ used in section 79 subsumes within it all kinds of
Internet service providers irrespective of what function they perform in the long
chain of intermediaries that transport Internet content to the desired destinations.
The ISPs perform different functions in the task of transporting content like
access providing, hosting and content providing and their liability cannot be
uniform. It has to be based precisely on what function they perform. It is
necessary to categorise the ISPs into functional categories otherwise different
ISPs could be held liable under the IT Act, 2000 for something which they have
played no role in or for the contents over which they have little control. To give a
meaningful disposition to the limitation on liability of ISPs, for which section 79
has been drafted, it becomes essential to categorise the ISPs. So, it is desirable
that in the IT Act various types of ISPs should be distinguished, depending upon
the specific functions they perform and their liability should also be fixed keeping
in mind the role they play in the overall transmission.

The title of section 79 of the IT Act “Network service providers not to be liable in
certain cases” makes apparent the object behind the section, which is to limit the
liability of ISPs. The liability of ISPs could arise in a number of ways under different statutes. The liability could be criminal or civil in nature depending on various factors. It is impractical to define the liability of ISPs which could arise in various forms at one place. Equally impractical could be to amend all our laws, which could hold ISPs liable, in order to limit their liability. The latter has not been attempted in any of the Indian legislations including the Copyright Act, 1957 till now. The IT Act, 2000 does not attempt the former but just seeks to create a filtering mechanism for determining the liability of ISPs. The idea is that the liability of an ISP for his action or omission be first determined in accordance with the statute under which it arises and then if at all the ISP is held liable, his liability again be filtered through section 79 of the IT Act. In this context, the expression “under this Act” which has been used in section 79 has created some confusion. Apparently, this limitation of liability would be applicable only when the liability has arisen under the IT Act alone. This could not be the motive behind drafting section 79 especially when the Act does not attempt to define the liability of ISP in any of its provisions; it only talks about limiting their liability. For the removal of doubts it is desirable that the expression “under this Act” be removed from section 79.

Section 79 of the IT Act provides two circumstances under which an ISP can qualify for exemption from liability. The first case is that of ‘knowledge’. Knowledge of the illegal contents on part of the ISP is a prerequisite for holding him liable under section 79 of the IT Act, 2000. The ISP can escape liability if it could be proved that he was unaware of all that was stored and passing through his servers. But if he is put under a notice that an infringing material is either stored or passing through his servers, he has to take proper action for removing or disabling that material otherwise he could be said to have knowledge of the infringing material and held liable. In this regard it is to be noted that ‘knowledge’ requirements for proving culpability in India differ from one field of law to another. But with regard to section 79 of the IT Act, which applies to any form of liability, the object of knowledge is not evident. Does it mean that the ISP has merely to
be aware of the content or he has to be aware of the illegality of the content as well? For example, a software product is stored on the servers of an ISP. To fulfil the knowledge requirement for holding the ISP liable, should he just know about the presence of the software or should he also know about its illegality. But especially copyright violations are often far from evident even if the ISP knows of the individual file on its server. To determine a file’s legality/illegality, the ISP needs to know not only the law but also additional facts on the creation of the work, the author, licences, individual contracts between the parties, etc. Should the ISP judge for himself whether that content is legal or not? This would be stretching his responsibilities beyond his capacity and capability. Should he employ legal specialists who judge the legality/illegality of the gigabytes present or passing through his servers? Even if he does so, the specialists' judgment could go ‘wrong’, as ultimately it is for the court to judge the legality. It is clear that upon obtaining knowledge as to the illegality of material an ISP has to remove it from its servers. It is very difficult for an ISP first, to be aware of all the files that are present or passing through its servers and second, to be certain about their legality/illegality. So how to induce ISP with the knowledge of the infringing material so as to make him liable? What is the exact way in which an ISP can be induced with such ‘knowledge’? This could best be achieved by notifying the ISP regarding the illegality of the material that is present or passing through his servers. The Act does not provide the acquisition of knowledge in any particular form contrary to what is contained in the DMCA. The legislator while drafting the IT Act, 2000 did not establish a notification procedure. But it can be considered implicit in the knowledge requirement because a takedown of infringing material can be effected by notifying the ISP, thereby inducing knowledge of the material as a prerequisite for liability under section 79 of the IT Act. On the one hand, lack of an official or formal notification procedure could induce the self-cleaning forces of the Internet, as anyone is free to notify the ISP, government agencies as well as copyright owners and third parties. But on the other hand, there are some drawbacks of not having any formal notification procedure as it can open the door to misuse through unsound and frivolous
takedown requests. It would mean that the ISP would have to remove the content on a mere notice by anybody? If that were so, he could enter in unnecessary confrontation with the person whose content he is hosting. A good example of notification procedure is that of the DMCA. Under the DMCA an intermediary must expeditiously block access to the information if he receives a notification of infringement. If an ISP were to take down material that turns out to be non-infringing, the Web site owner may have grounds to hold him liable for the damages suffered as a result of the removal of the material. Therefore, only if the ISP obtains this knowledge in a specific way, namely by receiving a notification that meets certain statutory requirements, will he incur liability. To limit this potential, some commentators are of the opinion that the notification has to be concrete enough in order to trigger the knowledge requirement; i.e. it must enable the ISP to easily find the content. And in the copyright setting they suggest that the notification contain factual data that allows the examination into existing copyrights. The ISP is only liable if the notice makes it aware of individual files and, in the copyright context, of additional facts sufficient to trigger the knowledge requirement. If it does so, the notice is justified. If, on the contrary, the notice is not definite enough, ignoring it does not trigger any liability, because the notice has not given enough facts to constitute knowledge of the ISP. Misuse through unsound takedown requests is thereby excluded. It is desirable that India should adopt within the IT Act, 2000 a notification procedure for ISPs to disable content. This would allow ISPs to disable specific content upon receiving specific information from specific persons and would provide ISPs definite circumstances under which they could disable potentially infringing material without being held liable for illegally removing the material. This would be in the interest of the copyright holders and ISPs both.

Apart from the knowledge requirement, for an ISP to escape liability, section 79 prescribes “due diligence” to be exercised by him. The provision requires actual knowledge or breach of the duty of care. What should be the extent of the “due diligence” requirement? Should the ISPs be required to monitor and judge
legality of millions of files that are present or passing through their servers? And what tools should they compulsorily employ for such an exercise? Why ISPs are unsuited to decide whether the alleged unlawful material should be taken down from the Internet and what are the consequences likely to follow from having ISPs making these choices and thus policing the Internet? Cases of copyright infringement are often not at all straightforward. Courts often struggle mightily with questions such as the following: Who owns the copyright? Has the duration of any copyright expired? Does the alleged infringer have a license to publish the allegedly infringing work? What is the scope and duration of any such license? Does the allegedly infringing act fall within any copyright exception or defence? Similar difficult legal and factual questions arise in cases involving defamation, fraud, misleading advertising, unfair competition, and the like. Complaints made to ISPs may not only be based on a good faith, but mistaken belief that one’s rights are infringed. While disputes about allegedly illegal material are often difficult even for courts to resolve, it goes without saying that ISPs are not at all well-equipped to deal with such issues.17 ISPs, as private providers of technical facilities, do not have the skills, knowledge, or personnel necessary to evaluate whether any particular material among the billions of bytes flowing over their facilities is infringing or illegal. In particular, this task may prove virtually impossible for the small ISPs that that comprise the Indian market. If knowledge of the mere existence of an individual copyrightable file were enough, ISP liability would be as vague and as wide as it were before the statutory limitation of section 79. The purpose of section 79 was to limit ISP liability. If an ISP would be under a duty to examine each file of third-party music, graphic or software, even with regard to circumstances that are not obvious from the file itself then we would be stretching the liability to the limits of sheer impracticality. Otherwise it would simply mean the end for many ISPs.

Technologies in the form of filtering and screening softwares that could be employed to check infringing material and facilitate the monitoring of the transmitted, cached or hosted content are available and will definitely undergo advancement in the years to come. What could be the impact of these technologies on such a duty of care? Consequently, the invention and application of monitoring technologies in the future may lead to greater liability. First, could the duty of care mentioned in the IT Act require ISPs to implement and operate filtering and control mechanisms? Second, could those ISPs who fail to implement such mechanisms be held liable for failure to comply with the mentioned duty of care? Third and more importantly, will ISPs be held liable if they fail to detect and remove material that, according to certain (yet undefined) standards, they should have been able to identify? Indeed, an aggrieved party could argue that the failure of an ISP to identify allegedly infringing material was due to a negligent implementation or operation of filtering mechanisms. Implementing these technologies could impose on the ISPs substantial costs and burdens. Considering the ISP sector in India, it may not be appropriate to burden ISPs with such technologies. Moreover, these technologies can never be fool proof. So there is a great dander of an ISP pandering to litigation because he, maybe in good faith, had disabled user’s content which was not infringing. So, in the interest of the growth of ISP industry in India the ISPs should not be burdened to implement these monitoring technologies. In this regard, ISPs should not be burdened with a duty to monitor the content which they transmit or store as this would amount to stretching their liability to the limits of impracticality. Therefore, the expression ‘due diligence’ occurring in the IT Act should be removed from section 79.

ISPs under various international statutes determining their liability are liable only if they are technically able and may reasonably be expected to prevent the use of illegal contents. The focus is on the reasonableness, because it will always be technically possible to stop access to illegal contents caused by the ISP – in the worst case simply by giving up all the services provided. Whether it may
reasonably be expected to bar use of illegal contents on the server may depend on whether it is technically possible to separate and remove the contents individually.\textsuperscript{18} This doctrine of reasonability and practicality is just not existent within section 79 of the IT Act and needs to be brought in as it would be futile to fix liability which cannot be reasonably fulfilled.

Under section 79 of the IT Act, the onus of proof lies on the ISP to prove any of the above two circumstances i.e. “knowledge and” “due diligence” to claim exemption from liability. The slippery wicket of burden of proof differs from statute to statute, depending on numerous factors. The expression used in section 79 of the IT Act “if he proves” imposes the burden of proving his innocence on the ISP in all circumstances and situations. This would be unfair to the ISPs considering that their liability could arise under various statutes of both civil and criminal nature. So, to be fair and logical this expression “if he proves” should be removed from section 79 of the IT Act and the rules for burden of proof need to be determined in accordance with the specific statute under which an ISP has been charged.

The liability of Internet service providers is one of the most controversial legal issues to emerge from cyberspace which is the result of the very nature of digital networks. Should ISPs be treated as electronic publishers, and thus made directly liable for all the infringing gigabytes flowing through their servers? Or are they merely the postmen of the Internet, common carriers exempt from all liability?\textsuperscript{19}

For the owners of intellectual property, it is practical to sue the ISPs as they are in a position of policing the Internet. On the other side of the argument, ISPs are passive carriers similar to telecommunications companies and therefore should


\textsuperscript{19} Kamiel Koelman and Bernt Hugenholtz, “Online Service Provider Liability for Copyright Infringement” OSP/LIA/1 Rev.1(1999) at p 3.
be granted some limitation from liability with regard to intellectual property infringement. The ISP industry is not unduly lucrative and in rural areas may have extremely tight profit margins, and any increase in the number of lawsuits or in the cost of providing service could lead many ISPs and telecommunications companies to decide not to provide Internet services in rural areas. The ISP industry should not be made a deep-pocket, third-party defendant in every online copyright infringement suit. Law’s lack of predictability in this area and its standards for ISP copyright liability over the past few years have caused real concerns for this new and growing industry. A narrow limitation on copyright infringement liability should be established for ISPs so that those who are building the Internet will have a clearer sense of how and when they might be held liable for online copyright infringement. A heightened level of certainty about their liability will help speed the growth of the Internet by encouraging more entrepreneurs to enter the ISP industry. Moreover, cooperation between ISPs and the content community is what is needed to address properly the issue of online copyright infringement.

Resolving disputes on the Internet involves determining jurisdiction and applicable law. In the world of pre-Internet, disputes were largely resolved through the traditional process of court litigation which is principally structured on a territorial basis i.e. each country has its own laws and courts, which decide disputes falling under their jurisdiction, mostly on the basis of the application of local laws. As long as the parties to a dispute arising on the Internet belong to the same jurisdiction, there is no problem, as the dispute in such a case would be solved in the same manner as any other offline dispute. For example, XYZ enterprises have their Web site through which they are selling goods manufactured by them. XYZ enterprises are based in Delhi and their customers are also in Delhi. In case any dispute arises between XYZ enterprises and their customer, it would be resolved according to the laws applicable in Delhi. But the problem would arise when their customers are from different countries and they are transacting with them through their Web site. This dispute resolution
mechanism based primarily on territoriality faces a number of challenges when applied to disputes arising on the Internet. The Internet is by definition International and can be accessed from almost any place on Earth hence multi-jurisdictional. On the Internet digitised data may travel through various countries and different jurisdictions in order to reach its destination. For example, a dispute may arise between two parties who entered into contract on the Internet and who belong to different countries. Now courts of which country should have jurisdiction to determine this dispute? The laws of which country should be relied upon to determine the dispute? These questions are perplexing even in the offline world and they become more accentuated in the online environment.

The digital technologies originated in the USA and not surprisingly, the earliest disputes arose in the USA as well. The fact that by far the US courts have the richest experience in tackling disputes arising in cyberspace induces us to look at how they are dealing with them. The US approach became very clear in a series of Internet related cases. By a number of decided cases a three-pronged test has emerged for determining whether the exercise of personal jurisdiction over a non-resident defendant is appropriate:

- the defendant must have sufficient (minimum contacts) with the forum state,
- the claim asserted against the defendant must arise out of those contacts, and
- the exercise of jurisdiction must be reasonable.  

‘Jurisdiction is proper [...] where contacts from actions by the defendant himself create a substantial connection with the forum state’. In an Internet context the real issue is whether making available a web site in the forum (and in the rest of the world) suffices to establish specific jurisdiction over a defendant and the cases arise

where the web site contains a trade mark that is allegedly reproduced there without the permission of the trade mark owner in the jurisdiction-place where the site is accessed. The Zippo court applied this rule to the Internet context and found that its review of the available cases ‘reveal[ed] that the likelihood that personal jurisdiction can be constitutionally exercised is directed proportionate to the nature and quality of commercial activity that an entity conducts over the Internet’.22 A passive web site that does little more than make information available to those who are interested in it is not a ground for the exercise of personal jurisdiction.23 This was, for example, the case when a Jazz club operated a web site that contained information about the venue and forthcoming events, but that did not offer visitor the opportunity to send e-mails or to make bookings.24 Things change when the site invites visitors to add their addresses to a mailing list. This was held to amount to a substantial connection because the conduct amounted to active solicitations and because every visitor received a reply.25 It suffices that the visitors of the site can contact the site-owner from the forum to establish a substantial connection.26 That shows that the defendant has taken deliberate action27 towards the forum. Similarly the combination of a web site and a newspaper add in a local paper to solicit funds established the necessary connection.28 A defendant that reaches intentionally beyond its boundaries to conduct business with foreign residents is subject to the exercise of specific jurisdiction. This was for example the case when Mr Patterson,

27 Ballard v. Savage, 65F. 3d 1495, 1498 (9th Cir. 1995).
a Texas resident, deliberately dealt with CompuServe in Ohio to upload his shareware software.29 In the Zippo case Zippo Dot Com had contacted 3000 individuals and seven Internet access providers in the Pennsylvania forum. This was sufficient in terms of contact to warrant the exercise of specific jurisdiction. The court pointed out30 though that ‘the test has always focused on the nature and quality of the contacts with the forum and not the quantity of those contacts’.31

The cases decided by the US courts, despite slight differences between them, show a clear and coherent approach adopted by the US courts in jurisdictional issues, even if the defendant deliberately avoids any personal contact with the jurisdiction. The approach in the EU countries is not as crystallised as we see in case of the USA. Though courts gradually are looking at the impact of the web presence of a business entity on the local jurisdiction along with their intention of entering into some sort of relationship.

As far as the criminal offences under the IT Act, 2000 are concerned, the position has been straightened by the Act which says that if the impact of a particular act is felt in India, Indian courts will have jurisdiction, thereby endorsing the ‘effect’ theory. Looking from a contractual perspective, the law is contained in the Code of Civil Procedure, which says that the jurisdiction lies where the cause of action, whether wholly or partly, arises. This principle would mean even if a part of cause of action has arisen within the precincts or the jurisdiction of an Indian court, the Indian court could exercise jurisdiction. Section 20 of CPC doesn’t talk about due process or minimum contact principles. So, under this theory mere Web site access could suffice for a court to assume jurisdiction. The moment a plaintiff shows that the Web site is accessible from India, he can show that a part of the cause of action has arisen here because Indian viewers are likely to view the

29 CompuServe, Inc. v. Patterson, 89 F. 3d 1257 (6th Cir. 1996).
Web site. Both the Copyright Act and the Trademarks Act say that the plaintiff can file a suit where he is located; he doesn't need to bother about where the defendant is located. This means Indian courts have a very wide jurisdiction as far as the Internet is concerned. But, despite a paucity of judicial guidance in this regard, we find that courts in India are, to a large extent, looking at something beyond mere access of a Web site.

With respect to intellectual property infringements on the Internet, the application of the above general principles often crystallizes in the question of whether the mere accessibility of a Web site in the territory is a sufficient basis for finding jurisdiction, or whether something more than mere accessibility is required. Generally, the mere accessibility of a Web site in a forum will not be deemed sufficient for a court to exercise jurisdiction over the defendant, but this position is not uniformly shared in all countries. Mere creation of a Web page anywhere in the world could potentially strike millions of individuals and businesses everywhere in the world. It would be unreasonable to suggest that this one act puts the owner of the Web site amenable to the jurisdiction of every court on the planet earth. This is a proposition which is correct neither theoretically nor practically or functionally.

The Internet operates in an environment, which allows infringements to take place with no clear and convenient jurisdiction in which the rightsholder can file suit. The challenge to the legal community posed by such an environment, is currently being dealt with at the national and international level. There has been an ongoing effort to form new rules that would apply to the online environment. They reflect a growing consensus that the principle of ‘freedom of contract’ should be accorded appropriate respect under the law as a means for facilitating electronic commerce. For the time being, in a complex international legal environment, a major role is played by private international law. Its role is to determine where one can litigate and which national law will apply to the various transactions. This means that existing tools are used to fill the vacuum. Where
the infringer is neither domiciled nor has his place of business or property within national territory, the rights holder has no choice but to enforce a judgment obtained within national territory in a foreign country. At regional level, there are proceedings for recognition of foreign judgments\textsuperscript{32}, but they are sometimes rather tedious and time-consuming. Consequently, steps should be taken towards creating an international convention for the recognition of foreign judgments, applicable throughout the world.

At the national level, the disputes are being settled through case-by-case determinations of the courts. The courts, however, face myriad, difficult factual circumstances, and must determine whether the exercise of jurisdiction is proper in situations where the relevant “contacts” with the forum have been through the network while the defending party is located in another state or country. Originally cyberlaw was not equipped at all to regulate transnational commercial transactions over the Internet and national laws were ill at ease in the digital borderless environment of the Internet. The courts around the world, not surprisingly, are struggling to come up with a coherent doctrine of personal jurisdiction for Internet transactions. It is probably far too early to suggest that concrete rules have yet emerged. Though, a few general themes appear to be emerging. Courts, by and large are looking at the contact, impact and effect of a particular Web site on local jurisdiction meaning thereby something more than a mere Web site access. It may take some time before a common understanding is achieved in the context of resolving disputes arising in cyberspace. In this regard it becomes important to highlight the role of judges. Intellectual Property is going to be the real estate of the third millennium. The Judges who have grown up with legal concepts shaped by traditional values will have to open up their minds to new ways of thinking about law and technology. The challenges posed by Internet and the digital medium are fascinating. What Justice Benjamin Nathan

\textsuperscript{32} The European Convention on Jurisdiction and Enforcement of Judgements and the Lugano Convention, which were concluded specifically in order to facilitate the enforcement of national judgments, at least within the EU and the EFTA.
Cardozo had to say about Judges facing a novel, unprecedented and un-patterned situation for which there was no legislation or settled case law is relevant at this juncture. To quote:\textsuperscript{33}

\begin{quote}
When the colours do not match, when the references in the index fail the serious business of a judge begins.
\end{quote}

Copyright is the child of technology. It was technology that necessitated the sprouting of copyright laws and every new technological innovation has lead the growth of copyright laws around the world. In the first place, every new technological invention threatened the survival of copyright industries and till now all the technologies have been assimilated into the copyright regime and the result is the manifold growth of copyright industries the world over. The traditional balance in copyright law has once again been altered by the development of digital and information technologies. The rise of the Internet has threatened the rights of copyright holders. The rising levels of piracy on the Internet has led to a debate about the future existence of copyright law.

Some people, like Nicholas Negroponte, head of the Media Lab of the Massachusetts Institute of Technology, think that the copyright system, as we know it actually, has come to an end.\textsuperscript{34} Others, on the contrary, are in favour of adapting the system to the new context originated by the new digital technologies. It is often postulated that copyright law has fallen hopelessly behind the explosive developments in technology and will, therefore, soon


become obsolete as a regulatory instrument in the digital world. Yet this prognosis appears unlikely, for a number of reasons:

- Copyright has by now a long tradition and has been well ingrained in the legal systems of almost all countries in all parts of the world. The present membership of 151 countries in the Berne Union is indicative of its wide acceptability and enormous contributions. The art industries have been legally, socially and economically sculpted by the presence of copyright.
- The copyright-based industries like, publishing, music, film, broadcasting, television, software, information, media and entertainment industries are among the largest in our society. Contributions of copyright industries amount to ‘huge sums’ to our corporate balance sheets every year and make a significant contribution to the national income statistics the world over. It is quite improbable that these giant multinational corporations will simply allow these billions to be smeared off their profit accounts. In other words, commerce will demand an evolution not a revolution.
- If history is some indicator of the unfolding of future events then it is worth considering. The phonogram didn’t kill the live performance industry as it was prophesied; the tape recorder didn’t kill the record business; television didn’t kill the cinema. All developments in the law of copyright are technology-driven and all significant changes in the copyright industries are similarly technology-driven. In the past copyright law has proved that it is flexible and open to reform in the face of technological advances.

Copyright must continue to play an essential role in any modern developed sophisticated society because at the end of the day, the rights of copyright are an award for innovation, creativity and risk taking and thus give a fillip to culture and the economy of our community. As stated by the U.S. Supreme Court, “From the

---

beginning, the law of copyrights has developed in response to significant changes in technology.\textsuperscript{36} The role of the legislature and courts, however, remain constant. They must maintain the delicate balance between the exclusive rights of copyright owners and the public’s right to have access to information. So, in the global digital economy our challenge is to ensure that the laws of copyright adapt to the new technological environment in a way that feeds and encourages creative activity rather than in a way that inhibits or overwhelms it. The proprietary aspect of copyright law is only one side of the matter, which is to be considered in close relation with its cultural-economic aspect.\textsuperscript{37} In other words, the right of copyright owners to equitable remuneration should always be balanced with the interests of society at large. The key is to balance which has always to be interpreted and reinterpreted considering varying interests from time to time along with the advancement of technology.


\textsuperscript{37} Ruth Towse, Creativity, Incentive and Reward (Edward Elgar Cheltenhorn UK 2001), p. 22 (...)}