# INFORMATION TECHNOLOGY ACT, 2000 AND THE COPYRIGHT ACT, 1957: SEARCHING FOR THE SAFEST HARBOR?

*Rajendra Kumar & Latha R Nair*[*]

*This paper seeks to assess whether the safe harbor provisions for Internet intermediaries as enacted in the Information Technology Act, 2000 and the amended Copyright Act, 1957, reflect a correct balance between content owners and users. The paper begins by tracing the history of the Internet in its Web 1.0 and 2.0 avatars. Further, it examines how the current Internet architecture has facilitated e-commerce transactions as well as social speech. Moreover, the paper discusses whether the standards of liability under the Information Technology Act for intermediaries reflect an internationally compatible 'notice-and-take-down-regime', thereby avoiding a situation which would effectively result in shooting the messenger. Moreover, it examines whether the standards of liability under the Indian Copyright Act, 1957 are consistent with those under the Information Technology Act, 2000. Lastly, it examines whether the Indian laws and judicial trends strike a fair and correct balance between right owners and users.*

## I. INTRODUCTION

The early Internet, also referred to as Web 1.0, was essentially static and did not permit any human interaction.[1] Users could only read or view information.[2] This information already existed in the analog world and the websites on the Internet simply replicated such information online.[3] For example, if one were to search for the details of a law firm in New York, the search would return a web page with information about the firm, its practice areas, the attorneys, their profiles etc. In other words, it was a uni-dimensional world with no window for interactive functionality. In contrast, the same website today, in addition to the above information, might offer a client access to his/her case status, provide a potential recruitee with a link to post his/her resume and even offer the possibility of an online interview!

The advent of high speed internet and broadband ushered in a platform where it became possible to share information and content in its

---

[*] The authors are partners with K&S Partners, a Gurgaon based IP law firm.

1 Umesha Naik & D Shivalingaiah, *Comparative Study of Web 1.0, Web 2.0 and Web 3.0*, available at http://ir.inflibnet.ac.in/bitstream/handle/1944/1285/54.pdf?sequence=1 (Last visited on May 21, 2013).

2 *Id*.

3 *Id*.

myriad forms, such as music, movies, images, files etc. Interactivity and collaboration became the two defining features of the Internet. The bulletin boards have rightly been considered to have heralded Web 2.0, in that these services enabled an interactive environment for its members to post their comments.[4] Unlike Web 1.0 where content posted on the World Wide Web engaged the users in a passive viewing experience, Web 2.0 comprises web applications that facilitate collaboration and sharing of information.[5] The user in a Web 2.0 environment became at once, a recipient and a creator of content in a virtual reflection of the real world. These inherent qualities of the Internet enabled websites to innovate and offer services such as hosting, linking, transmitting and indexing content, thereby revolutionizing the way we banked, listened to music, watched movies, learned and shopped for products and services in the virtual world. In other words, Web 2.0 changed the way the Internet had been hitherto understood and used.

## II. THE BIRTH OF E-COMMERCE AND USER GENERATED CONTENT ('UGC')

As a result of the collaborative and interactive functionality of Web 2.0 applications, it became possible for businesses and individuals to access, host and transmit third party content or services and conduct transactions on the Internet. Gradually, the real world business transactions started migrating to virtual platforms. At the social level, it became possible to connect with one's family and friends through these platforms.[6] The Internet steadily graduated to a virtual world with banks, markets, book shops, social networks, learning centers along with many other things.

The facilitators of such a virtual world are called 'internet intermediaries' because these entities distribute, host and help in locating online content.[7] A few examples of the intermediaries that are essential to the operation of e-commerce and social media networks are telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes (as given in the definition of 'intermediary' in the Information Technology Act, 2000[8] which broadly corresponds to the international understanding of the term).

By the very nature of their activities, Internet intermediaries carry content or provide services which may be fraught with legal liability,

4 Search CIO-Midmarket, *Bulletin Board System*, available at http://searchcio-midmarket.techtarget.com/definition/bulletin-board-system (Last visited on May 21, 2013).

5 Naik & Shivalingaiah, *supra* note 1.

6 *Id*.

7 OECD, *The Economic and Social Role of Internet Intermediaries*, April 2010, available at http://www.oecd.org/sti/ieconomy/44949023.pdf (Last visited May 27, 2013).

8 The Information Technology (Amendment) Act, 2008, § 2(1)(w).

i.e., the content may be defamatory, racist or published without permission of the owner of copyright or other intellectual property rights holder. In such instances, intermediaries run the risk of facing liability, both civil and criminal, for violation of intellectual property rights or other legal infractions such as defamation.

In one of the earliest U.S. cases, *Religious Technology Center* v. *Netcom On-line Communication Services, Inc*.,[9] ('Netcom case') the issue of liability of bulletin boards as a facilitator came up for consideration before a U.S. Court. In this case, the copyright holders (Religious Technology Center) brought copyright infringement action against the operator of a computer bulletin board (BBS run by one Mr. Thomas Klemesrud) and an Internet Service Provider (Netcom On-line Communication, Inc.), seeking to hold the defendants liable for copyright infringement committed by BBS subscribers/users. Dismissing the plaintiff's claim for direct copyright infringement against Netcom (the Internet service providers) as well as the BBS Operator, the District Court held as follows:[10]

> "This court is not persuaded by plaintiffs' argument that Netcom is directly liable for the copies that are made and stored on its computer. Where the infringing subscriber is clearly directly liable for the same act, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet. Such a result is unnecessary as there is already a party directly liable for covering the copies to be made. Plaintiffs occasionally claim that they only seek to hold liable a party that refuses to delete infringing copies after they have been warned. However, such liability cannot be based on a theory of direct infringement, where knowledge is irrelevant. The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred. Billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from non-infringing bits. Because the court cannot see any meaningful distinction (without regard to knowledge) between what Netcom did and what every other Usenet server does, the court finds Netcom cannot be held liable for direct infringement."

---

[9] Religious Technology Center v. Netcom On-line Communication Services Inc., 907 F.Supp.1361(N.D. Cal. 1995).

[10] *Id*., ¶ 23.

In an interesting footnote to the judgment, the Judge noted as follows:[11]

> "Netcom compares itself to a common carrier that merely acts as a passive conduit for information. In a sense, a Usenet server that forwards all messages acts like a common carrier, passively retransmitting every message that gets sent through it. Netcom would seem no more liable than the phone company for carrying an infringing facsimile transmission or storing an infringing audio recording on its voice mail. As Netcom's counsel argued, holding such a server liable would be like holding the owner of the highway or at least the operator of a toll booth, liable for the criminal activities that occur on its roads. Since other similar carriers of information are not liable for infringement, there is some basis for exempting Internet access providers from liability for infringement by their users."

This decision was delivered in 1995, even before the WIPO Internet Treaties were concluded in December 1996.[12] This was also before the U.S. Congress, taking cognizance of the difficult and controversial questions of copyright liability in the online world, passed the Digital Millennium Copyright Act ('DMCA') in 1998.[13]

## III. WHY NOTICE AND TAKE DOWN 'SAFE HARBOURS' FOR INTERNET INTERMEDIARIES?

The Netcom case described above is a seminal judgment as it presages the specific elements of an Internet intermediaries' claim for immunity from content liability, namely:

a. The intermediaries are mere common carriers/ messengers that passively retransmit every message that gets sent through them;

b. Their role in the transmission or storage or reproduction of the content is nothing more than setting up and operating a system that is necessary for the functioning of the Internet;

---

11 *Id,* ¶ 13.

12 WIPO, *The WIPO Internet Treaties,* available at http://www.wipo.int/export/sites/www/freepublications/en/ecommerce/450/wipo_pub_l450in.pdf (Last visited on May 21, 2013) (Refers to the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty as the 'Internet treaties').

13 U.S. Copyright Office Summary, The Digital Millennium Copyright Act, 1998, available at http://www.copyright.gov/legislation/dmca.pdf (Last visited on May 27, 2013).

c. They thus lack legal or actual control over the content that is transmitted through their servers;

d. It would be virtually impossible for them to manually check for the legality or otherwise of each file that passes through their servers or gets stored in their servers.

Besides the above mentioned arguments, the intermediaries have also argued that the very survival of e-commerce and the information society depends upon an immunity regime in which they are spared from liability on account of content generated or created by others. If it were otherwise, the intermediaries would be deterred and discouraged from participating and investing in e-commerce, because the burden and costs of liability exposure and monitoring content would make their business models economically unviable.[14] Such an eventuality would not be in public interest because it would discourage any further investment in the expansion of the Internet and the technologies that empower it.

As against the case for absolute immunity pleaded by the intermediaries, various governments and rights owners have argued that any such immunity would be an invitation to chaos; it would throw open the floodgates for dissemination of pornography, terrorism, libel or defamation and other forms of wrongful information.[15] As intermediaries are the only effective gate keepers to the Internet, it was argued that intermediaries could not shy away from sharing some of the responsibility in monitoring third party content.[16]

The 'notice and take down' regime was essentially a middle path solution between the two extremes, that is, absolute liability and no liability at all. The notice and take down regime proceeds on the basis that an intermediary is not liable for any third party content which passes through it or is stored by it on its servers, so long as it has no knowledge of the same. However, once it has gained knowledge of such content, it must act diligently to disable access or remove such content. Failure to act after taking cognizance would take away the safe harbor and expose the intermediary to liability. In one of the recent cases in Australia, Google Inc. as a search engine, was found to be a publisher of defamatory material and was denied the defense of innocent disseminator on grounds, *inter alia*, that it had been notified by the claimant of the defamatory nature of content and it failed to remove the same despite such notice.[17]

---

[14] Centre for Democracy and Technology, *Intermediary Liability: Protecting Internet Platforms for Expression and Innovation*, April 2010, available at https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf (Last visited on May 27, 2013).

[15] *See Id.*

[16] Lilian Edwards, *Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights*, available at http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf (Last visited on November 23, 2012).

[17] Trkulja v. Google Inc LLC (No 5), (2012) VSC 533.

# IV. STANDARDS OF LIABILITY FOR INTERMEDIARIES IN THE UNITED STATES AND EUROPE

The standards of liability for intermediaries worldwide have been influenced in some measure by the developments in the United States and Europe. In the U.S., copyright violations on the Internet are dealt with through a *sui generis* legislation namely, the Digital Millennium Copyright Act. Under the DMCA, the safe harbors exist for four specific types of activities performed by service providers, namely, (a) the provision of a network for transitory communications; (b) system caching; (c) storage of information on systems or networks at the direction of users and (d) information location tools.[18] The 'safe harbor' against copyright liability is available under the DMCA if an on-line service provider removes/disables access to allegedly infringing material, upon receiving a notice of infringement from a copyright owner or its agent in compliance with the statutory requirements under the DMCA.

As regards other types or forms of online content, there is a separate legislation in the U.S. called the Communications Decency Act. § 230(c) of this Act states that, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".[19]

The said section has become the bedrock of immunity for Internet service providers in the U.S. in respect of various legal wrongs, including defamation and obscenity.

On the other hand, Europe follows a uniform content-neutral approach to the liability of intermediaries (identified as the horizontal approach in the Council Directive).[20] The foundation of this approach is found in E-Commerce Directive 2000/31/EC ('E-Commerce Directive').[21] Articles 12 to 15 of the Directive[22] cover a range of intermediaries (referred to in the Directive

---

[18] The Digital Millenium Copyright Act, 1998, § 512.

[19] Communications Decency Act, 1996, § 230(c).

[20] Recital 16 of Council Directive 2001/29/EC of 22 May 2001.

[21] Directive 2000/31/EC of the European Parliament and of the Council, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML (Last visited on November 23, 2012).

[22] *Id*., Art. 12, 13, 14, 15.
Art. 12 - 'Mere conduit'
1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.

as 'information society service providers') in terms of their specific functions.

---

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this 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.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Art. 13 - 'Caching'

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
   (a) the provider does not modify the information;
   (b) the provider complies with conditions on access to the information;
   (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
   (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
   (e) the provider acts 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, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Art. 14 -Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
   (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
   (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Art. 15-No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate

Article 12 deals with intermediaries acting as 'mere conduits' and immunizes them from liability on the condition that the provider does not initiate the transmission, does not select the receiver of the transmission, and does not select or modify the information contained in the transmission. The 'conduit' safe harbor includes telecommunications carriers, Internet access providers and other backbone services that are central to the functioning of the Internet. This standard seems to be an absolute standard because it is not conditional on any notice and take down regime. However, Article 12(3) of the E-Commerce Directive engrafts a limitation on the conduit safe harbor, as it preserves the possibility for a court or an administrative authority, in accordance with Member States' legal systems, to require the service provider to terminate or prevent an infringement. In *Twentieth Century Fox Film Corporation* v. *British Telecommunication PLC* ('British Telecommunication case'),[23] the High Court of England and Wales was confronted with the question of whether the absolute immunity granted under Article 12 (1) of the E-Commerce Directive could be limited by a requirement in terms of Article 12(3) by ordering the ISP concerned to terminate or prevent an infringement. The factual matrix in which this controversy came to be adjudicated before the High Court related to a website, www.newzbin2.com, which could be accessed by U.K. users through British Telecom's (BT) services. The claimant Studios sought an injunction against BT to require it to terminate the infringement complained of. It was beyond doubt that the Newzbin2 website was a pirate and rogue website which knowingly allowed its subscribers to access pirated copies of the claimant Studios' films/ TV shows. It was BT's contention that the Court had no jurisdiction to pass the order sought, because such an order would contravene the mere "conduit" safe harbor provided for in Article 12(1) of the Directive.[24] The High Court agreed with BT's submission that it is protected from liability for infringement of copyright by Article 12(1) of the Directive. However, the High Court held that, "Article 12(3) provides that this protection does not 'affect the possibility for a Court…of requiring a service provider to terminate or prevent an infringement'."[25]

BT argued that the order sought by the claimant Studios was designed to disable access to information, which could not be imposed under Article 12(3) but only under Article 14(3), which was applicable to hosting services. Rejecting this argument, the High Court held:[26]

> "*First*, Article 12(1) places no limit on the type of injunction that may be granted "requiring a service provider to terminate or prevent an infringement". *Secondly*, the part of

to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

23 Twentieth Century Fox Film Corporation v. British Telecommunication PLC, (2011) EWHC 1981.

24 *Id.*,¶ 98, ¶159.

25 *Id.*, ¶159.

26 *Id.*,¶ 160.

> Article 14(3) relied on by counsel for BT is not concerned with court orders, but with administrative procedures established by Member States, such as a 'notice and take down' procedure operated by an administrative body. Indeed, the part of Article 14(3) that relates to court orders has the same wording as Article 12(3). *Thirdly*, Article 14(3) must be read in the context of Article 14 as a whole. Article 14 is concerned with service providers who act as "hosts", that is to say they store information provided by a recipient of the service. In those circumstances, it is understandable why Article 14(3) refers to the establishment of procedures for the removal or disabling of access to such information. This does not justify a restrictive interpretation of Article 12(3). *Fourthly*, recital (45) of the E-Commerce Directive says that injunctions against intermediary service providers can consist of "orders by courts…requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it". This makes it clear that Article 12(3) should be interpreted as extending to orders requiring service providers to disable access to illegal information."

In contrast to the 'mere conduit' safe harbor, the safe harbors for 'caching' services are available for the automatic, intermediate and temporary storage of information. Further, these safe harbors are conditional on their ability to act expeditiously, to remove or disable access to the information stored by them, upon obtaining knowledge. The knowledge here refers to the fact that the information at the initial source of the transmission has been removed from the network or access to it has been disabled, or a court/an administrative authority has ordered such removal or disablement. Similarly, 'hosting' services enjoy immunity from liability so long as the provider does not have actual knowledge of the illegal activity or information or upon obtaining such knowledge or awareness, the service provider acts expeditiously to remove or disable access to the information.

It is clear from the above brief review that while the E-Commerce Directive confers complete protection to mere conduits (subject to conditions imposed by courts), it posits a 'notice and take down' approach to hosting and caching services. Search engines are not expressly included in the safe harbor provisions under the E-Commerce Directive. Accordingly, individual EU Member States are free to apply their own laws to deal with the liability of search engines. However, emerging case law in Europe has extended the scope of the Directive to search engines or online market places.

In *Google Inc* v. *Louis Vuitton*,[27] Louis Vuitton submitted that a referencing service such as AdWords was not an information society service within the terms of the provisions of Directive 2000/31, with the result that the provider of such a service could not under any circumstances avail itself of those restrictions on liability. Google and the Commission of the European Communities took the opposite view. Disagreeing with the submissions made by Louis Vuitton, the European Court of Justice held as follows:[28]

> "Article 14 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') must be interpreted as meaning that the rule laid down therein applies to an Internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned." (Emphasis supplied)

In *L'Oreal* v. *Ebay*,[29] the European Court of Justice was invited to answer a reference, among others, whether the service provided by the operator of an online marketplace is covered by Article 14(1) of Directive 2000/31 (hosting), and if so, in what circumstances it may be concluded that the operator of such online marketplace has 'awareness' within the meaning of Article 14(1) of Directive 2000/31. Answering the reference in favour of online market places, the Court held as follows:

> "Article 14(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') must be interpreted as applying to the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored.

---

[27] Google Inc. v. Louis Vuitton, C-236/08, Judgement of the Court (Grand Chamber), March 23, 2010.

[28] *Id*., 121.

[29] L'Oreal v. Ebay, C-324/09, Judgment of the Court (Grand Chamber), July 12, 2011.

> The operator plays such a role when it provides assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them.
>
> Where the operator of the online marketplace has not played an active role within the meaning of the preceding paragraph and the service provided falls, as a consequence, within the scope of Article 14(1) of Directive 2000/31, the operator none the less cannot, in a case which may result in an order to pay damages, rely on the exemption from liability provided for in that provision if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of Directive 2000/31." (Emphasis supplied)

Article 15 of the Directive mandates that Member States shall not impose a general obligation on service providers, when providing the services covered by Articles 12 to Article 14, to monitor the information which they transmit or store, nor a general obligation to seek facts actively or circumstances indicating illegal activity. In *Scarlet Extended SA* v. *SABAM* ('SABAM case'),[30] decided by the European Court of Justice, the dispute involved a collective society, SABAM, and an Internet service provider, Scarlet, which provided its customers access to the Internet without offering other services such as downloading or file sharing. SABAM contended that Internet users using Scarlet's services were downloading works in SABAM's catalogue from the Internet, without authorization and without paying royalties, by means of peer-to-peer networks. SABAM sought an order requiring Scarlet to bring such infringements to an end by blocking or making it impossible for its customers to send or receive files containing a musical work, using peer-to-peer software without the permission of the right holders. The Court of Appeal, Brussels, posed to the ECJ the following reference for interpretation of the Directive:[31]

> "Do Directives 2001/29 and 2004/48, in conjunction with Directives 95/46, 2000/31 and 2002/58, construed in particular in the light of Articles 8 and 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that: 'They [the national courts] may also issue an injunction against intermediaries whose services are used by a

[30] Scarlet Extended SA v. SABAM, Case C-70/10, Judgement of the Court (Third Chamber), In Case C-70/10, November 24, 2011.

[31] *Id.*,¶ 28.

> third party to infringe a copyright or related right', to order an [ISP] to install, for all its customers, in abstract to and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing *via* its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent?" (Emphasis supplied)

The Court noted that implementation of a filtering system of the kind sought by SABAM, would require the ISP to identify within all of the electronic communications of all its customers, the files relating to peer-to-peer traffic. Further, within that traffic, the ISP would be required to identify the files containing works, in respect of which holders of intellectual property rights claim to hold rights, determine which of those files are being shared unlawfully and then block such file sharing. The Court found that such preventive monitoring would require active observation of all electronic communications conducted on the network of the ISP concerned and consequently, would encompass all information to be transmitted and all customers using that information. The Court held that:[32]

> "In the present case, the injunction requiring the installation of the contested filtering system involves monitoring all the electronic communication made through the network of the ISP concerned in the interest of those right holders. Moreover, that monitoring has no limitation in time, is directed at all future infringements and is intended to protect not only existing works but also future works that have not yet been created at the time when the system is introduced.
>
> Accordingly, such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its business since it would require that ISP to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual property rights should not be unnecessarily complicated or costly." (Emphasis supplied)

[32] *Id.*,¶ 47, 48.

# V. STANDARDS OF INTERMEDIARY LIABILITY IN INDIA

## *A. THE INFORMATION TECHNOLOGY ACT*

In India, the Information Technology Act, 2000 ('IT Act') was enacted in 2000 to give a fillip to the growth and usage of computers, Internet and software in the country as well as to provide a legal framework for the regulation of e-commerce and e-transactions in the country. A key part of the IT Act relates to the provision of 'safe harbors' to intermediaries. The definition of 'intermediary' in the IT Act reads as follows:

> "Intermediary" – with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.[33]

§ 79 of the IT Act, exempted network service providers from liability in certain cases and reads as follows:

> "Section 79: For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, Rules or Regulations made thereunder for any third party information or data made available by him if he proves that the offense or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offense or contravention.
>
> *Explanation*:—For the purposes of this section—
>
> a) "Network Service Provider" means an intermediary;
>
> b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary."

§ 81 of the IT Act contained a non-obstante clause and provided that the provisions of the Act would have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.[34]

In *Firos* v. *State of Kerala*,[35] the High Court of Kerala was dealing with the effect of § 81 of the IT Act (as it existed then) in relation to a right

[33] The Information Technology (Amendment) Act, 2008, § 2(1)(w).

[34] Information Technology Act, 2000, § 81: Act to have overriding effect: The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

[35] Firos v. State of Kerala, AIR 2006 Ker 279.

claimed under the Copyright Act, 1957 ('Copyright Act') in respect of a computer program.

The Division Bench of the High Court of Kerala held:[36]

> "All matters connected with copyrights can be resolved by the provisions in the Copyright Act as it is a special Act for that purpose and matters regarding information technology have to be resolved by applying the provisions of the Information Technology Act as it is a special Act for that purpose."

The effect of the above judgment is that the rights under the Copyright Act are not affected by the non-obstante provision of § 81 of the IT Act, in so far as these rights are owned by independent authors and do not constitute government works. If any act of the Government under the IT Act had the effect of interfering with or taking away any of these rights, the Copyright Act would have precedence over the IT Act, and it would be open to any aggrieved person to challenge such act as arbitrary. The above judgment of the Kerala High Court is currently under appeal before the Supreme Court of India.

In 2008, the IT Act underwent a batch of amendments. The Report of the Expert Committee on the Proposed Amendments to the IT Act, 2000 (August 2005),[37] *inter alia*, explains that the provisions relating to intermediary liability have been revised to expressly elucidate the extent of liability of an intermediary in certain cases. The Report acknowledges that the EU Directive on E-Commerce 2000/3/31/EC issued on June 8, 2000 has been used as guiding principles.[38]

The provisions relating to 'intermediary' (definition of 'intermediary', safeguards applicable to them) and § 81 thereof were amended to the following effect:

> § 2(1)(w)[39] — "Intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

---

[36] *Id.*,¶4.

[37] Report of the Expert Committee, *Proposed Amendments to Information Technology Act, 2000*, August 2005, available at http://www.prsindia.org/uploads/media/Information%20Technology%20/bill93_2008122693_Report_of_Expert_Committee.pdf (Last visited on November 14, 2012).

[38] *Id.*

[39] Information Technology (Amendment) Act, 2008, § 2(1)(w).

§ 79:[40] Exemption from liability of intermediary in certain cases:

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf

(3) The provisions of sub-section (1) shall not apply if-

(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation:—For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

§ 81. Act to have overriding effect:- The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

[40] *Id*., § 79.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957) or the Patents Act, 1970 (39 of 1970).

Pursuant to § 79(2)(c) of the amended IT Act, the Central Government issued the Information Technology (Intermediaries Guidelines) Rules, 2011 on April 13, 2011.[41] These Guidelines require intermediaries to observe due diligence while discharging their duties by taking the following steps:

(i) To publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person;

(ii) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that –

a. […]

b. Is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling or otherwise unlawful in any manner whatsoever unlawful;

c. […]

d. Infringes any patent, trademark, copyright or other proprietary rights.

The above Rules further clarify that certain actions by an intermediary shall not amount to hosting, publishing or storing of any such information, namely:

a. Temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

b. Removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorized by the intermediary pursuant to any order or direction as per the provisions of the Act.

[41] G.S.R. 314(E), April 11, 2011, available at http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf (Last visited on November 20, 2012).

The Rules require that the intermediary, on whose computer system the information is stored, hosted or published, upon obtaining knowledge by itself or through an affected person in writing or email signed with electronic signature about any such information, shall acknowledge the complaint within 36 hours. Further, wherever applicable, the intermediary must work with the user or owner of such information to disable information that is in contravention of sub rule 2. The intermediary shall redress such complaints promptly, within one month from the date of its receipt.[42] Further, the intermediary shall preserve such information and associated records for at least 90 days for investigation purposes. As per Rule 3(11), each intermediary is also required to publish on its website, the name of the Grievance Officer and his contact details, and 'the mechanism' by which users or any person who is affected can submit their complaints. The Grievance Officer must redress the complaint within one month of the date of receipt of the complaint.

In *Google India Private Limited* v. *M/s Visaka Industries Limited*,[43] the High Court of Andhra Pradesh had the occasion to deal with the applicability of the safe harbors under § 79 of the IT Act as described above. In this case, certain politicians had complained that some articles available on Google had defamed them. Despite having been notified, Google India Private Limited ('Google India') did not remove access to these articles. Google India relied upon the defense of safe harbor under §79 and claimed immunity. The Court, however, did not agree with Google India and held as follows:[44]

> "It is only under the said amendment, non-obstenti (sic) clause was incorporated in Section 79 keeping application of other laws outside the purview in a fact situation covered by the said provision. Now, after the amendment, an intermediary like a network service provider can claim exemption from application of any other law in respect of any third party information, data or communication link made available or hosted by him; provided he satisfied the requirements under Sub-section (2) of Section 79. Further, as per amended Sub-section (3) of Section 79, the exemption under Sub-section (1) cannot be applied by any Court and cannot be claimed by any intermediary in case the intermediary entered into any conspiracy in respect thereof. Also, the intermediary cannot claim exemption under Sub-section (1) in case he fails to expeditiously remove or disable access to the objectionable material or unlawful activity even after receiving actual

[42] Ministry of Communications and Information Technology, Government of India, Issue of Clarification, March 18, 2013, available at http://www.naavi.org/importantlaws/it_rules_compendium/Clarification%2079rules_1_18mar13.pdf (Last visited)

[43] Google India Pvt. Ltd. v. M/S Visaka Industries Ltd and Anr., Crl. P. No. 7207 of 2009 (Andhra Pradesh H.C).

[44] *Id.*, ¶3.

> knowledge thereof. In the case on hand, in spite of the 1st respondent issuing notice bringing the petitioner about dissemination of defamatory material and unlawful activity on the part of A-1 through the medium of A-2, the petitioner/A-2 did not move its little finger to block the said material or to stop dissemination of the unlawful and objectionable material. Therefore, the petitioner/A-2 cannot claim any exemption either under Section 79 of the Act as it stood originally or Section 79 of the Act after the amendment which took effect from 27.10.2009."

The case is currently under appeal before the Supreme Court of India. In this context, it is submitted that, examined purely in the light of the relevant section of the IT Act, it would appear that the judgement of the High Court of Andhra Pradesh could not be faulted.

## *B. THE COPYRIGHT ACT*

Before the amendments to the Copyright Act in June 2012, there were no specific provisions dealing with the issue of intermediary liability under the Act. § 14 of the Copyright Act sets out the exclusive rights conferred upon the owner of the copyright in the protected categories of copyright works.[45]

§ 51 of the Copyright Act sets out two categories of liability for copyright infringement, namely, 'primary infringement' and 'secondary infringement'.[46] In *Super Cassettes Industries Limited (SCIL)* v. *MySpace*

---

[45] The Indian Copyright Act, 1957, § 14: For the purposes of this Act, "copyright" means the exclusive right subject to the provisions of this Act, to do or authorise the doing of any of the following acts in respect of a work or any substantial part thereof, namely:-
(a) in the case of a literary, dramatic or musical work, not being a computer programme, -
(i) to reproduce the work in any material form including the storing of it in any medium by electronic means;
(ii) to issue copies of the work to the public not being copies already in circulation;
(iii) to perform the work in public, or communicate it to the public;
(iv) to make any cinematograph film or sound recording in respect of the work;
(v) to make any translation of the work;
(vi) to make any adaptation of the work;
(vii) to do, in relation to a translation or an adaptation of the work, any of the acts specified in relation to the work in sub-clauses (i) to (vi);
(b) in the case of a computer programme,-
(i) to do any of the acts specified in clause (a).

[46] The Indian Copyright Act, 1957, §51: When copyright infringed - Copyright in a work shall be deemed to be infringed -
(a) When any person, without a licence granted by the owner of the copyright or the Registrar of Copyrights under this Act or in contravention of the conditions of a licence so granted or of any conditions imposed by a competent authority under this Act-
(i) does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright, or

*Inc.*,[47] a Single Judge Bench of the High Court of Delhi had the occasion to examine the liability of a social networking website, MySpace, under the rubric of primary and secondary infringement. The Single Judge interpreted the exclusive rights conferred on the owner of copyright under §14 of the Copyright Act to include the right to 'authorize' the doing of such acts. Based on such an interpretation, the Judge agreed with MySpace that infringement by authorization required that the person charged had the authority, or the right to ask that an act of actual breach of copyright be committed. Thus, the Court found that SCIL had not established *prima facie* that MySpace exercised such degree of control amounting to approval, countenance or sanction on its part. However, the Single Judge held MySpace liable for secondary infringement under §51(a)(ii)[48] of the Copyright Act, taking into account the following factors:

a) The provision of "notice and take down" safeguards on MySpace's website is proof of its reasonable apprehension or belief that the acts on its website may infringe someone else's copyright;

b) Reasonable belief or knowledge specific to SCIL's works is present since SCIL had supplied its name and lists of titles owned by it to MySpace. Further, MySpace had been dealing with SCIL prior to the institution of the suit. MySpace could not be oblivious to the fact that the Bollywood songs which were going to be performed on its website may belong to SCIL and SCIL had notified MySpace time and again about its updated works;

c) Knowledge and reasonable belief can be seen when one examines the working mechanism of MySpace. MySpace takes a limited license from the user to amend, delete or modify the works suitably. For the same, the works go into the servers or the computers of MySpace when the programmers modify, or amend the said content suitably. The said modification goes to the extent of adding advertisements and logos of other companies prior to or after the clips;

d) Knowledge and reasonable belief is also apparent when MySpace indulged in India-centric operations wherein a whole office was dedicated to Indian works catering to Indian consumers;

---

(ii) permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he was not aware and had no reasonable ground for believing that such communication to the public would be an infringement of copyright…

Explanation – For the purposes of this section, the reproduction of a literary, dramatic, musical or artistic work in the form of a cinematograph film shall be deemed to be an "infringing copy".

47 Super Cassettes Industries Ltd. v. MySpace Inc., CS (OS) No. 2682/2008 (Delhi H.C).

48 § 51(a) (ii) :"…permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he was not aware and had no reasonable ground for believing that such communication to the public would be an infringement of copyright".

e) § 51(1)(b) does not permit post-infringement due diligence.

MySpace's defense under § 79 of the IT Act (in its current form)[49] also failed because the Judge found that § 81 of the IT Act excludes copyright and patents from its purview. However, the Judge went on to examine the defense of safe harbors under § 79 and held it to be inapplicable because he found that MySpace's functions were not confined only to providing access to a communication system where third party information is stored, transmitted or hosted. The Judge took the view that MySpace provides access only after a limited license to add or modify the works, thereby adding advertisements to the said works.[50] Consequently, the Judge found post infringement measures to be an insufficient safeguard against the rights of SCIL.

The Single Judge's order is under appeal before a Division Bench of the High Court of Delhi. After the amendments in June 2012, § 52 of the Copyright Act,[51] has been amended to provide for exceptions to copyright infringement in respect of the following specific acts, namely:

> "…
>
> (b) the transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public;
>
> (c) transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder, unless the person responsible is aware of or has reasonable grounds for believing that such storage is of an infringing copy;
>
> Provided that if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work, complaining that such transient or incidental storage is an infringement, such person responsible for the storage shall refrain from facilitating such access for a period of 21 days or till he receives an order from the competent court refraining from facilitating access and in case no such order is received before the expiry of such period of 21 days, he may continue to provide the facility of such access."

In keeping with the aforesaid amendments, § 14 of the Copyright Act in respect of cinematograph films and sound recording works, has been

---

[49] *See* Information Technology (Amendment) Act, 2008, § 79.

[50] Super Cassettes Industries Ltd. v. MySpace Inc. & Anr, CS (OS) No. 2682/2008 (Delhi H.C.),¶ 46.

[51] The Indian Copyright (Amendment) Act 2012, § 52.

amended to provide an additional right of storage of such works in any medium by electronic or other means.[52]

The Standing Committee Report on the Copyright Amendment Bill, 2010 in relation to the proposed amendments to § 52, noted the submissions of the Department of Higher Education, Ministry of Human Resource Development which were as follows:[53]

> "According to the Department, Section 52 deals with fair dealing and certain acts which are not infringement and it does not deal with infringement per se. Any transient and incidental storage of any work through the process of 'caching' has been provided exceptions as per the international practice. Any deliberate storing of such works and unauthorized reproduction and distribution of such works is infringement under Section 51 of the Act attracting civil and criminal liability…The proposed amendments in clause (c) introduces (sic) liability of Internet service providers. The practice of making available the works on Internet and websites in unauthorized manner without license from the author or right owner is infringement. This leads to suspension of the service provider's activity. However, in order to provide a safe harbor as per international norms to the service provider to take down such unauthorized works upon receipt of notice from the authors and right owners and any abuse of suspension, it is provided that an order within 14 days from the competent court to be produced for the continued prevention of such storage."

Yahoo India submitted that:[54]

> "…the proposed amendments have been loosely worded and may not specifically cover certain areas such as search, hosting, information retrieval and caching…The Copyright Act should clearly specify that an ISP will be liable only if it has knowledge of the infringing activity and has failed to

---

[52] The Indian Copyright Act (Amendment) Act, 2012, §14(d):
In the case of a cinematograph film,—
(i) To make a copy of the film, including—
A. photograph of any image forming part thereof; or
B. Storing of it in any medium by electronic or other means
(ii) To sell or give on commercial rental or offer for sale or for such rental, any copy of the film
(iii) To communicate the film to the public.

[53] The Parliamentary Standing Committee Report on the Copyright Amendment Bill 2010, available at http://copyright.gov.in/Documents/227-Copyrightamendment.pdf (Last visited on November 20, 2012).

[54] *Id.*,¶ 19.4.

> remove the infringing material on receiving notice from the concerned content owner or if it induces, causes, or materially contributes to the infringing conduct of another. The Act should clearly define the extent and parameters of ISP liability otherwise (sic) every ISP is subject to unlimited liability for third party actions. It is submitted that ISP should not be held responsible for words, pictures and videos that they did not create and before an ISP is held liable an effective Notice and Take Down (NTD) mechanism should be followed. NTD is a kind of self regulatory measure where parties hosting content agree to remove content in case of a legitimate notice by content owner. Further, criminal liability in case of infringement of copyright should apply to direct infringers and not to ISPs which merely provide the platform or means of communication for the end users."

The right owners opposed these amendments on the ground that it would make it very easy for any online pirate/ person to make infringing digital copies and get away with such conduct by pleading that the storage was incidental while in the process of transmission. In view of the divergent views expressed by the stake holders, the Standing Committee was of the view that the viability of the 14 days period needs to be reviewed.[55] The Committee further recommended that the words, 'transient and incidental' should be replaced in both the clauses so as to read 'transient or incidental', in order to take care of the concern expressed by ISPs for unlimited liability due to third party actions.[56]

Viewed in the light of the submissions made before the Committee and its recommendations, it would appear that the legislative intent behind the amendments in § 52 was to primarily provide safe harbors to various ISPs, though the language of the amendments does not expressly convey the same. In the absence of policy considerations for exclusion of any given category of intermediaries, such an interpretation would be consistent with the treatment of intermediaries under the IT Act. Under §79 of the IT Act, the safe harbors have been incorporated to cover and immunize various kinds of intermediaries, and the notice and take down regime is the condition for continued applicability of such safe harbors. There are, however, certain differences in the standards of intermediary liability under the two statutes. It may be noted that the predecessor section to the current § 79 of the IT Act placed on the intermediary, the onus of proving lack of knowledge and exercise of due diligence to prevent the commission of the offense or contravention complained of.[57] The case of

---

[55] *Id.*,¶19.10.

[56] *Id.*

[57] Information Technology Act, 2000, § 79: Network service providers not to be liable in certain cases- "For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence

*Avnish Bajaj* v. *State*,[58] illustrates how the predecessor section was applied by the High Court of Delhi in refusing to quash the criminal proceedings initiated against Avnish Bajaj for liability under § 79. The Supreme Court of India[59] has overturned the Delhi High Court's finding with regard to Avnish Bajaj's liability, on the grounds that § 85 of the IT Act should be read as stating that a director could not have been held liable for the offence under § 85 and that accordingly, the proceedings against Avnish Bajaj were liable to be quashed. The Supreme Court further held that as far as Mr. Bajaj's company was concerned, it was not arraigned as an accused and therefore, the proceeding in the existing incarnation was not maintainable either against the company or against Mr. Bajaj, its director.

As against the regime applicable under the un-amended IT Act, the safe harbors under the current § 79 are available automatically. The intermediaries lose immunity on failing to expeditiously remove or disable access to unlawful material, after receiving actual knowledge or being notified by the appropriate government or its agency of the same, and if the intermediary has conspired, abetted, aided or induced the commission of the unlawful act. In other words, the elements of active participation of the intermediary in the acts complained of and its failure to act after knowledge are the *sine qua non* for the liability to arise under the IT Act.

In contrast to these standards of liability under the IT Act, § 52(1) (b) of the Copyright Act seems to provide absolute immunity to intermediaries whose functions include the transient or incidental storage of a work or performance, purely in the technical process of electronic transmission or communication to the public.[60] The exception would appear to apply to conduit functions *akin* to the conduit exception under the European E-Commerce Directive, and would relate to telecommunications carriers/ Internet access providers.

The exception under §52(1) (c) would appear to cover other kinds of intermediary functions such as search engines, caching, hosting, payment gateways, e-commerce intermediaries.[61] However, the immunity offered to such intermediaries is available so long as there are no circumstances which show that the intermediary concerned is aware, or has reasonable grounds for

---

or contravention was committed without his knowledge or that he had exercised all the due diligence to prevent the commission of such offence or contravention".

58 Avnish Bajaj v. State (N.C.T.) of Delhi, 116 (2005) DLT 427.

59 Avnish Bajaj v. State (N.C.T) of Delhi, Cri. App. No. 1483 of 2009.

60 Indian Copyright (Amendment) Act, 2012, § 52 (1)(b): the transient or incidental storage of work or performance purely technical in process of electronic transmission or communication to the public.

61 Indian Copyright (Amendment) Act 2012, §52 (1)(c): transient or incidental storage of work or performance for the purpose of providing electronic links, access or integrations, where such links, access or integration has not been expressly prohibited by the right holder, unless the person responsible is aware or has reasonable grounds for believing that such storage is an infringing copy.

believing that such storage is of an infringing copy. By its very nature, this condition would necessitate either actual knowledge or constructive knowledge, based on the circumstances which would show that the service is being used to store infringing copies. In this context, websites like Newzbin in the British Telecommunication case discussed above would fail to avail themselves of immunity from liability. In addition to the presence of actual or constructive knowledge, the section has a proviso which requires the right owner to notify the intermediary in writing of the infringing works, and obliges such owner to obtain an order from the competent court during a period of 21 days from the date of such notification. If there is a court order within the said period, the intermediary responsible must refrain from facilitating such access. If no such order is received within the said period, the intermediary may continue to provide such access.

The difference in the treatment of intermediaries under these two sub sections lies in the nature of the services being carried out by them. While the intermediaries covered under §52(1)(b) are the core backbone service providers whose functions are integral to the internet, those covered under §52(1)(c), distribute, host and help in locating online content. The latter category constitutes the pith and substance of e-commerce and thus requires a certain legal regime where the intermediaries are encouraged to invest in the growth of e-commerce in exchange for certain safe harbors against liability for online content.

## VI. WHETHER INDIAN LAWS AND JUDICIAL TRENDS REFLECT A CORRECT BALANCE BETWEEN RIGHT OWNERS AND USERS?

In *R Rajagopal* v. *State of Tamil Nadu*,[62] the Supreme Court of India was confronted, *inter alia*, with the question whether the freedom of press guaranteed by Article 19(1) (a), entitles the press to publish unauthorized accounts of a citizen's life and activities and if so, to what extent and in what circumstances. The observations of the Supreme Court are as under:[63]

> "As far as the freedom of press is concerned, it flows from the freedom of speech and expression guaranteed by Article 19(1)(a). But the said right is subject to reasonable restrictions placed thereon by an existing law or a law made after the commencement of the Constitution in the interest of or in relation to the several matters set out therein. Decency and defamation are two of the grounds mentioned in clause (2). Law of torts providing for damages for invasion of the right

[62] R. Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264.
[63] *Id.*,¶ 21.

> to privacy and defamation and sections 499 / 500 IPC are the existing laws saved under clause (2). But what is called for today in the present times is a proper balancing of the freedom of press and said laws consistent with the democratic way of life ordained by the Constitution. Over the last few decades, press and electronic media have emerged as major factors in our nation's life. They are still expanding and in the process becoming more inquisitive. Our system of government demands as do the systems of governments of USA and UK constant vigilance of exercise over governmental power by the press and the media among others. It is essential for a good government."

In the context of copyright law, the Supreme Court has emphasized the same need for balance of these competing interests in *M/S Entertainment Networks* v. *Super Cassettes*:[64]

> "The Act seeks to maintain a balance between the interests of the owner of the copyright in protecting his works on the one hand and the interest of the public to have access to the works, on the other. The extent to which the owner is entitled to protection in regard to his work for which he has obtained copyright and the interest of the public is a matter which would depend upon the statutory provisions. Whereas the Act provides for exclusive rights in favour of owners of the copyright, there are provisions where it has been recognized that public has also substantial interest in the availability of the works…".

The above noted position by the Supreme Court echoes the position of the ECJ in the SABAM case discussed above, that the rights available under intellectual property laws are not absolute rights and it needs to be balanced against the countervailing need for public access to information.

On May 16, 2011, the report of the Special Rapporteur of the United Nations on the Promotion and Protection of the Right to Freedom of Opinion was presented to the Human Rights Council of the General Assembly. The report explores the role of intermediary liability and states as follows:[65]

> "Intermediaries play fundamental role in enabling Internet users to enjoy their right to freedom of expression and access to information. Given their unprecedented influence over

[64] M/S Entertainment Networks Ltd. v. Super Cassettes, 2008(9) SCR 165,¶ 61.

[65] United Nations General Assembly, Human Rights Council [UNHRC], Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, ¶ 74, 75, U.N. Doc. A/HRC/17/27 (May 16, 2011).

> how and what is circulated over the Internet, States have increasingly sought to exert control over them and to hold them legally liable for failing to prevent access to content deemed to be illegal.
>
> The Special Rapporteur emphasizes that censorship measures should never be delegated to private entities, and that intermediaries should not be held liable for refusing to take action that infringes individuals' human rights. Any requests submitted to intermediaries to prevent access to certain content or to disclose private information for strictly limited purposes, such as administration of criminal justice, should be done through an order issued by a Court or a competent body which is independent of any political or commercial or other unwarranted influences."

Judged in the light of the aforesaid law laid down by the Supreme Court of India and the international norms advocated by the United Nations, it would appear that the current judicial trends in India do not always reflect the much needed balance between the need for protection of copyright and the need for public access to information. The spate of John Doe orders passed by various High Courts of India in the recent past at the instance of copyright owners of cinematograph films, illustrates how the Courts have passed wide ranging orders against intermediaries, directing them to block or disable access to websites, which may potentially carry third party generated infringing content. The scope of such orders is open ended and applies indiscriminately to all the intermediaries arrayed before the courts without regard to the functions played by them. This places them with an impossible task of installing a complicated, costly and permanent computer system to monitor without any limit in time, the existing works as well as future works.

This is illustrated by an order of the High Court of Madras in *RK Productions Private Limited* v. *BSNL*,[66] passed on April 25, 2012, where the film producer sued a number of intermediaries including BSNL, Bharti Airtel, Vodafone, MTNL etc, and obtained an order of injunction against all of them, restraining them from infringing the plaintiff's copyright in the film '3'.[67]

Aggrieved by the said order, a number of intermediaries challenged it before the Division Bench of the High Court of Madras, primarily on the ground that the nature of the injunction granted by the Single Judge

[66] R.K. Productions Pvt. Ltd. v. BSNL, C.S. No. 208/2012 (Madras H.C) (Unreported).

[67] *Id*("…by copying, recording, reproducing, or allowing camcording or communicating, or allowing others to communicate or making available or distributing, or duplicating, or displaying, or releasing or showing or uploading or downloading or exhibiting or playing in any manner communicating the plaintiff's movie '3' without a proper license from the plaintiff … through different medium including CD/ DVD/ blue ray disc, VCD, cable TV, direct to home services, internet services, multimedia messaging services…").

did not take account of the role played by these intermediaries. Clarifying the order passed by the Single Judge, the Division Bench held on June 22, 2012 as follows:[68]

> "The order of interim injunction dated 29.3.2012 and 25.4.2012 ….are hereby clarified that the interim injunction is granted only in respect of a particular URL where the infringing movie is kept and not in respect of the entire website. Further, the applicant is directed to inform the respondents/ defendants about the particulars of URL where the infringing movie is kept and on such receipt of particulars of URL from the Plaintiff/ applicant, the Defendants shall take necessary steps to block such URLs within 48 hours."

Despite the clarification given by the Division Bench, a number of intermediaries in the suit sought vacation of the interim injunction order passed earlier on March 29, 2012, *inter alia*, on the ground that the functions of the intermediaries consist primarily in providing access to the Internet and it would be virtually impossible on their part to monitor all the data and information that pass through their servers.

The Single Judge upheld[69] the maintainability of a John Doe suit in terms of the principles laid down in *ESPN Software India Private Limited* v. *Tudu Enterprise*,[70] which had held that the Indian courts have jurisdiction to pass an order against unknown persons arrayed as Ashok Kumars. The Judge further noted that the order passed by him on March 29, 2012 was subsequently clarified by the Division Bench in the order dated June 22, 2012. Since the amended order was not under challenge and the arrangement worked out in the said order was a workable solution without hurting the stand of either party, the Judge proceeded to dispose of the intermediaries' challenge in terms of the amended order already granted.

The above order was apparently passed under the Copyright Act as it existed before the amendments in June 2012. The Court did not have the occasion to consider the exceptions to copyright infringement under § 52(1)(b) & (c). As noted above, the exception under §52(1)(b) seems to provide an absolute safe harbor to such intermediaries which are involved in the transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public. In the judgment referred to above, BSNL and Bharti Airtel Limited would qualify as such intermediaries

---

[68] Unreported order passed by the Division Bench of the High Court of Madras on June 22, 2012 as reproduced in the order of the Single Judge of the High Court of Madras in Suit No. CS 208/2012 and CS No. 294/2012.

[69] Unreported judgment passed by the High Court of Madras on October 30, 2012 in Suit No. CS 208/2012 and CS No. 294/2012.

[70] ESPN Software India Pvt. Ltd. v. Tudu Enterprise, CS (OS) No. 384/2011 (Delhi H.C).

providing conduit functions. It is a moot point whether the order passed by the Single Judge of the High Court of Madras on October 30, 2012 would be consistent with the said exception today, as any immunity granted to such intermediaries under this section should be absolute. In other words, the Court should have looked at the nature of functions of these intermediaries (all of which appear to be mere conduits) while arriving at its conclusions. Surprisingly, the defendants did not rely on this exception under the amended Act.

## VII. CONCLUSION

The judicial trends discussed above reflect an insufficient understanding of how the Internet functions, especially the facilitating role played by various intermediaries in providing access to the Internet. More importantly, it is unclear as to why the standards of intermediary liability under the Copyright Act do not mirror those under the IT Act. The policy considerations underlying both the statutes are based upon a balance between two competing interests, that is, the public interest in the dissemination of information which is central to the Internet and the public interest in the protection of third party rights including intellectual property rights. On the one hand, the safe harbor provisions under § 79 of the IT Act, vest a right of censorship in the hands of private intermediaries which act at the instance of any person or government agency, more out of fear of losing the safe harbors than any objective assessment of the legality or otherwise of the complaints received.[71] This would be contrary to the views advocated by the United Nations that such requests "should be done through an order issued by a Court or a competent body which is independent of any political or commercial or other unwarranted influences".[72] On the other hand, the safe harbors under § 52(1)(c) leave the question of their application to specific intermediaries, to the vagaries of interpretation and judicial intervention. Either way, the situation does not help the cause of the intermediaries and the rights of the users. Unless redressed at the legislative level, it may unwittingly lead to the shooting of the messenger itself, thereby sabotaging the robust growth of the digital world.

---

[71] *See* Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, April 10, 2012, available at http://cis-india.org/internet-governance/intermediary-liability-in-india (Last visited May 30, 2013).

[72] *Supra* note 65.