Liability of Intermediaries in India — From troubled waters to safe harbors

By Apar Gupta*

Cite as: (2007) PL May 3

1. Introduction

1.1. The Baazee case, an illustration of onerous liability imposed in a lacuna of safe harbors

Harvard educated Avnish Bajaj, Chief Executive Officer of US-based auction portal eBay's Indian subsidiary, baazee.com, would have never imagined that he would be spending his days lodged inside Jail No. 3 inside Delhi's Tihar Prisons with about 70 other undertrials accused of crimes ranging from pick-pocketing to rape and murder. Mr Bajaj was arrested after a video clip containing objectionable matter showing two Indian teenagers was offered for sale at Baazee.com. His liability stemmed from the fact that his website was allegedly publishing prohibited electronic content under existing laws in India. The outrage caused by his arrest was voiced from eBay, to Colin Powell, the then Secretary of State of the United States of America, NASSCOM ostensibly the parens paternae of software firms in India and civil society in general. This case demonstrates the dangers faced by intermediaries which are clear and present. This article, examines the contours of liability which an intermediary faces, in the absence of adequate safe harbor protections and addresses the legal lacuna which must be filled, taking into view the report submitted by the Expert Committee on review of the Information Technology Act, 2000.

2. Definition of parameters

2.1. Types of intermediaries

The architecture of the Internet aids the dissipation of content inherently promoting the role of intermediaries as the distributors of content. At a basic level, the Internet's technology requires the insertion of intermediaries between interacting parties in two ways. First, for all interactions over the Internet, the communication necessarily involves the Internet itself, as well as the parties necessary to facilitate the particular communication, with the exception of few entities involved in direct Internet transmissions, secondly, commercial transactions on the Internet require the use of other intermediaries. This part cannot hope to provide an exhaustive list of all the intermediaries that facilitate Internet content distribution but will provide four broad categories based on functionalities, in which present as well as future intermediaries may be pigeonholed. It is to be stated at the very outset that a single entity may fall into two or more categories dependent on activities, which it undertakes.

2.1.1. Communications gateway provider

The nomenclature herein will include any service provider that acts as a gatekeeper allowing primary access to data over the Internet. Though the term is inclusive of the Internet Service Providers (ISP) it is not synonymous with it and includes Network Service Providers (NSP) and Wi-Fi hotspots providers. Courts have taken the position that ISPs are companies or corporations that enable clients to connect to the
2.1.2. Permanent data hosts
A permanent data host is a much broader category and refers to any permanent web address for data uploaded by a user that is accessed by connecting to the Internet. The Internet is an open network of interconnected computers. The architecture of the Internet requires that for every website whose domain is registered, an assigned web host should be present, which contains the data stored on a server, kept continually online. It is important to differentiate this from file linking where merely a link of file is provided, as opposed to the file itself. The nature of data hosted may be of any kind ranging from a few lines of text posted in an online forum or web blog to a photograph or a music file uploaded by a user on a server.

2.1.3. Transitory data hosts
As opposed to a permanent data host a transitory data host is an intermediary which acts, as a “passive conduit” for data as it moves from one point on a network to another, thus enabling users to post content on the Internet. A service provider is covered under this category for it transmits, routes or provides connections for content through its system or for transient storage of content in the course of transmitting, routing or providing connections. This would include a POP3 email host which stores messages on its servers till they are downloaded on the user’s computer when he accesses his email through an email client as well as caching of web pages by ISPs.

2.1.4. Linking and referring intermediaries
Referring or linking intermediaries refer or link users to an online location by using information location tools, including hyperlinks and directories. Conceptually, a link is comprised of three parts, a source anchor, a destination anchor, and a direction. The document containing the link is the link’s source anchor; the link targets or points the user to the destination anchor. The target page can be any kind of resource.


2.2. Types of liability

Liability is dependent on the capacity of the actor against whom the liability is sought to be imputed. The Internet can potentially impose all three types of liability on an intermediary, which include, (1) direct; (2) vicarious; and (3) contributory liability.

2.2.1. Direct liability

A message posted on a usenet group is copied by thousands of servers owned by different parties who participate in distributing such messages automatically. If a usenet message includes copyrightable material without the permission of the copyright owner, the owner of servers might be liable for direct copyright infringement by permitting a copy of the message to be copied on their servers. In Netcom case it was stated that direct liability should require some additional act by the alleged infringer that is absent when copies are made automatically by a server. The Court stated that direct infringement is ordinarily inappropriate because the designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it. In Ellison v. Robertson the Court rejected the plaintiff's demand to impose direct liability on America Online, an ISP, for copyright infringement by a fan, who uploaded his favorite author's novel to a newsgroup on the Internet. Accordingly, direct liability is seldom alleged against intermediaries since the very architecture of the Internet involves them de minimis.

2.2.2. Vicarious liability

Indirect liability consists of two branches, vicarious liability and contributory infringement. Vicarious copyright infringement initially was conceived as an outgrowth of the agency principles of respondeat superior. Vicarious liability constitutes a form of enterprise liability that holds the defendant liable for the behavior of another. Vicarious liability would


require that the defendant and the infringer have an apparent or actual partnership, having authority to bind another in transactions with third parties or exercise joint ownership or control over the infringing product. Vicarious liability is imposed even if the entity is unaware of the infringing activities. With regard to copyright infringement, vicarious liability arises when the defendant possesses the right and ability to supervise the infringement conduct and has an obvious and

direct financial interest in the exploitation of copyrighted materials. In Playboy Enterprises, Inc. v. Frena the court found a Bulletin Board Service (BBS) operator vicariously liable for permitting the unauthorised uploading of images from the plaintiff’s magazine to the Internet for commercial gain. Under the Fonovisa test, the first prong of vicarious liability, namely, financial interest, can be satisfied by showing that the infringing uses of a technology act as a draw for customers, or in other words, enhance the attractiveness of a venue.

The second prong, the right and ability to supervise direct infringers, can be established by relying on findings that the defendant reserved its right to block its service to any consumer at will. Thus,

35. Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143 (7th Cir. 1992) at 1150.


38. See Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263-64 (9th Cir. 1996). See also Netcom, supra fn 28 at p. 1375 citing Shapiro, Bernstein & Co., fn 38 at p. 306.


vicarious liability was enforced against a website owner and operator where he owned the website, held a position of supervisory authority over the website operations, had the right and the ability to exercise control over the website’s infringing activities, and received a direct financial benefit from the website. Generally, most schools and corporations have the right, but not the ability, to supervise their Internet users’ activities effectively. Georgia Institute of Technology’s spokesperson, Bob Harty, stated, “Our experts advise us that it is all but impossible to effectively block access to a single site, without dramatically disrupting access to the entire Internet.” Hence, to advocate vicarious liability for large intermediaries would be erroneous.

2.2.3. Contributory liability

Specifically, the doctrine of contributory infringement arises out of the theory of enterprise liability. It states that liability should attach whenever a person knowingly contributes to the illegal conduct of another. In the Internet world, contributory liability will attach if a party knows, or reasonably should know, of infringing activities occurring on the party’s website, and the party materially contributes to the infringement. Contributory liability with regard to copyright infringement over the Internet may be used here as laying down the parameters for contributory liability where it is found that an intermediary, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another. The second prong of contributory infringement is sometimes analysed as substantial participation.

Courts have found the required level of contributory infringement knowledge satisfied in a variety of different ways, including: specific notice of infringement; the abnormally low price of the infringing goods; unusual business arrangements with the direct infringer; to the infringement activity induces, causes or materially contributes to the infringing conduct of another. The second prong of contributory infringement is sometimes analysed as substantial participation.


Contributory liability was imposed on BBS operators where they provided the facilities, knowledge, direction, and encouragement for the infringing conduct to occur, despite lacking knowledge of precisely when unauthorised copies were downloaded from or uploaded to their BBS by Internet users.64 Participation in or contribution to the infringing conduct was satisfied where a service provider knew that infringing material was posted on its network and yet allowed the information to be stored on its servers for distribution to other servers.65 Defendants also induced or materially contributed to the infringement when they encouraged users to upload files and, as a result, benefited from the extensive databank they accumulated for their subscribers to use.66

2.3. Standards of liability
Existing liability schemes generally join traditional fault-based liability and strict liability rules with broad Internet-specific liability exemptions. Those exemptions, the viability of the regimes is examined below

2.3.1. Fault liability
Mann & Belzley have given an illustration of a fault based regime as when, â€œ[T]he primary malfeasor is the actor who can most efficiently prevent Internet-related misconduct. When an Internet worm is released onto the Internet, for example, the


person who can most easily prevent the harm is the person who wrote the worm and released it.\footnote{67} A fault liability regime would imply that an act or omission renders an intermediary liable as a contributory since it is not the primary actor in the illegality. Mr Fulton has drawn a link between the fault of Netcom to make its policy on \#$\text{Intellectual Property Rights on the Internet}\$# readily available in the wake of the Netcom decision as an omission giving rise to possible contributory liability based on fault on grounds of non-publication of its hosting policy.\footnote{68}

2.3.2. Strict liability

Strict liability flows on the ipso facto finding of a cyber wrong, committed by an entity through an intermediary.\footnote{69} Under a strict liability approach, the traditional product, sale and defect requirements of products liability law would be relaxed so that those who commercially disseminate information or ideas embodied in books, magazines, records, CDs, movies, radio or television broadcasts, video cassettes, computer programs, or who make information or ideas available to the public over the Internet, would be potentially subject to liability as product sellers.\footnote{70} Both direct and vicarious liability regimes are examples of strict liability, which does not require that the alleged infringer have knowledge of the infringement.\footnote{71} It has been stated that imposing strict liability on ISPs for third-party defamation and copyright infringement would lead to ISPs gradually going out of business due to adverse judgments or policing costs necessary to keep infringing material off their systems.\footnote{72} This poses a threat to affordable information access.\footnote{73}

In Religious Technology Center v. Netcom On-Line Communications Services, Inc. the court stated, \#$\text{it does not make sense to adopt a rule [of strict liability like that in Frena] that could lead to the liability of countless parties whose role in infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet.}\$#\footnote{74} Here the court recognised that maintaining a strict liability standard would hold the entire Internet liable simply because of the architecture of the Internet.\footnote{75} Hence the policy of holding intermediaries strictly liable, as policy Judge Learned Hand once deemed \#$\text{harsh}\$# and worthy of \#$\text{hesitat[ion]}\$# would be unpragmatic

3. Lex Lata — The prevailing safe harbors

Black\textsuperscript{\textindex{Black\textsuperscript{\textindex{Law Dictionary}}%{Law Dictionary}#{Law Dictionary}}} defines a \#$\text{safe harbor as [a provision (as in a statute or regulation) that affords protection from liability or penalty]}\$# and an intermediary bereft of it is susceptible to a liability thicket. The rationale for providing Internet intermediaries safe harbors is that given the obvious technical and economic impracticalities, intermediaries cannot be expected to monitor or regulate (particularly on an ongoing basis) the vast amount of content which they host on their servers for their subscribers nor the phenomenal amount of material that is transmitted through the Internet each day.\footnote{76} The Information Technology Act of 2000 provides some shelter for intermediaries based on a combined, knowledge and due diligence standard.\footnote{77} This part presents and analyses the ambit of the safe harbors and the requisites to be satisfied by an intermediary under the present law.
3.1. The extent of the safe harbors
The extents of the safe harbors allowed under the Act are limited. Firstly, with regard to the subject-matter providing an
ambiguous definition as to intermediaries, not defining the scope and exposing intermediaries to possible litigation.
Secondly, it limits the extent of the safe harbors to “this Act, rules or regulations made thereunder” leaving intermediaries
vulnerable to civil and criminal liability flowing from the provisions of other enactments. It has been noted in this respect
that, “it appears to move India some, but

78. Cheng Lim Saw & Winston T.H. Koh, â€œDoes P2P have a Future? Perspectives from Singaporeâ€•, 13 Intâ€™l J.L. & Info
Tech. 413, 418 (2005).
79. Information Technology Act, Ch. XII, Section 79 (2000) (India) available at
80. Ibid.
only some, steps toward the convergent standards for ISP liabilityâ€•81.

3.1.1. Ambiguity in defining intermediaries
The safe harbors provided under the Information Technology Act, 2000 apply only to â€œnetwork service providersâ€•. It is
further provided that a â€œnetwork service provider[s]â€• is an â€œintermediaryâ€•82. An â€œintermediaryâ€• is defined as, â€œ
particular electronic message mean any person who on behalf of another person receives, stores or transmits that
message or provides any service with respect to that messageâ€•83. The flaws with the section are as follows

82. Information Technology Act, supra fn 79, Section 79 Explanation (a).
83. Information Technology Act, supra fn 79, Section 2(w).

(1) Knowledge of the architecture of the Internet shows that not all network service providers are intermediaries and not
all intermediaries are network service providers. Examples include obvious ones such as credit validation, and non-
obvious ones such as online mediation, negotiation, arbitration, collection and others84. The absence of this knowledge
acts as an obvious exclusion of benefit of safe harbors to these intermediaries against the spirit of the enactment. It is
imperative to have a definite definition as to intermediaries which is absent under the Act85.

(2) Moreover, the definition of an intermediary is only operational with respect to a â€œmessageâ€•. The term is not defined
throughout the breadth of the Act. Though a message may be defined
84. Sankar Virdhagriswaran et al, â€œTwo Level Architecture for Web Service Interactions Position Paper to Workshop on
Web Servicesâ€•, available at http://www.w3.org/2001/03/WSWS-pop/ paper49 (last visited 29-3-2006). See also Aashit
85. Asian School of Cyber Laws, â€œRecommendations made to Government of India for Amendments to the Information
visited 29-3-2006).

as, â€œA unit of communication exchanged between equivalent network layers or services, located at different hosts86â€•
several interpretations are possible.

(3) The scope of the provision is further shrouded when the degree to which the activities of, â€œreceiptâ€•, â€œstorageâ€• and
â€œtransmissionâ€• receiving safe harbors is not specified. Hence, ambiguity prevails as to whether a permanent host or a
transitory storage host or both would be covered by the definition. The definition obviously excludes linking and referring
intermediaries, which would leave intermediaries like Bazee bereft of safe harbor protections. The only plausible rationale
behind the exclusion is shoddy drafting when such intermediaries enjoy safe harbors in similar legislations87.

3.1.2. Limited safe harbor protection
A key defect of the Act is that the above defence applies only to offences under the Act and not to offences under other
laws88. In a case against Rediff.com India Limited an Indian search portal a Magistrate found sufficient evidence of
violation of Section 292 of the Indian Penal Code, 1860 to begin trial of Directors of a company whose on-

86. Brian Lavoie & Henrik Frystyk Nielsen, â€œWeb Characterization Terminology & Definitions Sheetâ€• (24-5-1999), available
https://www.supremecourtcases.com
Eastern Book Company
Generated: Wednesday, May 6, 2020
at http://www.w3.org/1999/05/WCA-terms/(last visited 29 3 2006).


line service allows users to find other websites by means of a search engine, some of which may be containing pornography. In Bazeed case Mr Avnish Bajaj is charged under Section 67 of the Information Technology Act, 2000 and Sections 292, 294 and 439 of the Penal Code, 186090. Thus, the statutory protection provided proves inadequate.

3.1.3. Burden of proof
The statute states that, â€œno person providing any service as a network service provider shall be liable â€¦ if he proves placing the burden of proof on the intermediary to preclude liability. This provision seeks to adopt the approach of the Digital Millennium Copyright Act, 2000. Where the availability of the limitation on remedies or â€œsafe harborâ€• under Section 512 is an affirmative defence, as to which the defendant bears the burden of proof.93

3.2. Prerequisites to be satisfied for precluding liability

3.2.2. Absence of knowledge


91. Information Technology Act, supra fn 79, Section 79.

92. Digital Millennium Copyright Act, supra fn 87, Sections 512(a) and (c).

93. ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 626 (4th Cir. 2001). See also Laura Rybka, Als Scan, Inc. v. Remarq Communities, Inc.: Notice and ISPâ€™s Liability for Third Party Copyright Infringement, 11 DePaul-LCA J. Art & Ent. L. 479, 484 (2001).

This provision appears to adopt the contributory liability standard for imposing liability upon intermediaries when knowledge of the illegal activity renders the intermediary liable. However, the section is silent as to whether â€œknowledgeâ€• is actual knowledge or constructive knowledge. The differing approaches as to actual or constructive knowledge can lead to varying results. An illustration is the finding of the District Court in the Sony case that Sony had no direct involvement with Video Television Recorders purchasers and so was not involved in a possible infringing use of the product. Although its advertising material made no mention of copyright law, Sonyâ€™s Video Television Recorders instruction manual warned purchasers that unauthorised copying of television programs and content could be a breach of the copyright law. The court assumed that Sony had constructive knowledge that its machines could be used to record copyright material but this fact alone was insufficient for it to be liable as a contributory infringement of copyright. Thus, it is imperative to define the standard of knowledge.

3.2.3. Exercise of due diligence to prevent offence
The second circumstance precluding liability of an intermediary is that, â€œthat he had exercised all due diligence to prevent the commission of such offence or contravention. There exist different standards for due diligence, which include (1) absolute due diligence, and (2) personal due diligence.


95. Information Technology Act, supra fn 79.


The section nowhere provides by way of an explanation what constitutes due diligence or enumerates criteria therein. Thus at best the safe harbor provided to intermediaries under the Information Technology Act, 2000 proves sketchy and inadequate.
4. Lex ferenda â€“ the proposed safe harbors

An expert committee was shortly appointed to review the working of the Information Technology Act with the objective of curing its obvious defects. It submitted its report, which included a draft for amendments in the Information Technology Act, 2000. This section analyses the draft amendments to the Act, which are principally aimed to remove the anomalies and ambiguities in the provisions of the Act. With respect to intermediaries, two sections are sought to be amended by the draft, (a) the definition of intermediaries to remove ambiguity, (b) the substantive safe harbor provisions under Section 79 to extend the exemption from liability.

4.1. Removal of ambiguities

The scheme of the Act disposes of the nomenclature of a “network service provider” only making an exception to liability for an “intermediary”. The term “intermediary” has been redefined with the term “messages” being substituted for “electronic records”. Electronic records have further been defined in the draft, as “data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche”.

The draft amendments further provide illustrations of intermediaries as including but not limited to, “telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines including online auction sites, online market places, and cyber cafes”. These sections cumulatively remove the ambiguity that surrounds the present enactment. However, the ingenuity of the Internet to devise novel forms of intermediary activity may cause hardship to future intermediaries. An illustration is an email to snail mail service such as the “epost” where printed or even handwritten messages of customers are scanned and transmitted as email through Internet. At the destination offices, these messages are printed, enveloped and delivered through postal workers like other letters at the postal addresses. These activities obviously fall outside the scope of an “electronic record” and thus an exception for an intermediary from liability is unavailable under the Act.

4.2. Adoption of the horizontal approach

The present provisions have been criticised on grounds of it applying only to offences under the Act and not to offences under other laws. The draft seeks to cure this by providing that, “an ‘Intermediary’ shall not be liable under any law for the time being in force”.

Moreover, this approach is relatively technologically sound because the information that travels through online intermediary facilities such as cables, satellites and servers is just a sequence of bits, a succession of zeros and ones which is not linked to the real meaning of the information itself. Thus, no longer intermediaries may be threatened with prosecution under statutes such as the Penal Code, 1860.

105. See Cabell, supra fn 88.

106. Proposed Amendments to the IT Act, 2000, supra fn 99, Section 79(1).
4.3. Prerequisites for seeking to preclude liability
The prerequisites to be satisfied for precluding liability, which are based on the premise of an entity claiming exception from liability in the draft provision is (a) an intermediary (b) claims an exception with respect to third party information, data, or link. Third-party information has been explained as any information dealt with by an intermediary in his capacity as an intermediary. On the satisfaction of these prerequisites, an intermediary can generally obtain exemption from liability.

4.4. Prerequisites for seeking to impose liability
The due diligence provisions in the present enactment have been dispensed with in the proposed amendments. However, there is a disqualification from exception of liability based on conspiracy or abetment by the intermediary of the illegal act. Moreover, when on (a) receiving actual knowledge; or (b) on notification by the Central Government or its agency, that (a) any information, data or link residing on a computer resource controlled by the intermediary is being used to commit an unlawful act; and (b) the intermediary fails expeditiously to remove or disable access to that material on that resource, the intermediary cannot avail the exception from liability.

The first notable feature of this proposed sub-section is that it relies upon actual knowledge, clearly defining the standard of knowledge required. Actual knowledge here means the receipt of information from a third party, but not from own inquiry upon the content of the information. Though the procedure for an intermediary acting on a notification by the Central Government is absent in the proposed amendment and that may further expose intermediaries to liability from aggrieved parties when it has been proven that the content was neither illegal nor harmful. The procedure should include requirements such as, the notification must be in writing, signed, sufficiently identify the allegedly infringing material, contain the address of the complaining party and a statement that that party has a good faith belief that the use of the material is contrary to law.

The proposed sub-section adopts a contributory liability regime where the mere factum of control over an information, data or link being used to commit an unlawful act does not make it liable. Here control should be coupled with the fault of the intermediary in expeditiously removing or disabling access to that material.

4.5. Specific provision for communications gateway providers and transitory data hosts
The proposed amendments provides a specific provision for intermediaries giving access to a communication network over which information made available by third parties is transmitted or temporarily stored. This provision is based on the EU Directive on Electronic Commerce. The application of the general exception of liability is including but not limited to this class.

The provision states that where such an intermediary does not, (a) initiate the transmission i.e. the provider does not
make the decision to carry out the transmission; (b) select the receiver of the transmission; and (c) select or modify the information contained in the transmission, the intermediary shall not be liable. However, clause (c) does not provide that an intermediary selecting or modifying the information does not include manipulations of a technical nature occurring in the course of the transmission, since such manipulations do not alter the integrity of the information contained in the transmission.119 It is quite peculiar that the proposed amendments do not specifically provide for provisions for permanent data hosts and linking and referring intermediaries.

4.6. Liability for breach of confidentiality and privacy
The draft amendments propose insertion of a specific provision to protect the identity of subscribers to the services of an intermediary. For the application of this section, the intermediary should (a) gain access to any material or other information relating to a subscriber who avails his services; (b) discloses such information or material to any other person; (c) without the consent of such subscriber; and (d) with intent to cause injury to him.120 The penalty imposed for such a breach of confidentiality and privacy is damages by way of compensation not exceeding Rs 25 lakhs.

We have recently witnessed corporate entities, particularly marketing and

119. Ibid. at Article 12(1)(c).
120. Proposed Amendments to the IT Act, 2000, supra fn 99, Section 72(2).

advertising companies, ãœharvestingâ€• or acquiring information on individuals, often without their consent, and on behalf of others. This has led to both legitimate and illegitimate practices in the acquisition, usage, storage and trading of such information.121 It has been stated that on the Internet, nobody knows you are a dog122 and this proposed section seeks to preserve the principle of anonymity inherent in Internet communications.

5. Conclusion
The Internet has continually expanded over the past decade, becoming an invaluable medium for communication on a global level. As Adam Smith noted human beings have, ãœthe natural propensity to truck, barter, and exchange one thing for anotherâ€•123 the use of the Internet as a tool for commerce was soon discovered. The passage of time has seen the growth of intermediaries as well as the functions performed by them. However, this growth is being threatened by imposing liability on them when they act as a mere conduit comparable to traditional facilitators such as postal services and telephone directories.

In the application for grant of bail of Mr Avnish Bajaj, the Delhi High Court granting him bail observed that, ãœ[T]his case will indubitably bring to the fore the dangers endemic in this business, which must be addressed forthwith.â€•124 Though the

122. Peter Steiner, The New Yorker, 5-7-1993, at 61.
124. Avnish Bajaj, supra fn 90 at p. 365.

proposed amendments substantially address these dangers and reduce the ambiguities in the definitions, providing for a scientific and horizontal level of protection, they still are inadequate. They do not provide for specific provisions for permanent data hosts or linking and referring intermediaries.

Whether these proposed amendments adequately balance the rights of the injured party and the intermediary is a question that can only be addressed through application. However, one answer is forthcoming that the amendments are better if not perfect than the provisions of the present enactment.

Â
Â