INTERMEDIARY LIABILITY IN THE CYBER SPACE WITH REFERENCE TO THE IT ACT 2000: A CRITICAL ANALYSIS

Ashabari Basu Thakur*1

ABSTRACT

The tremendous growth of the internet has brought in the concept of intermediaries. The intermediaries store, receive and transmit the record of any information. This has called for attribution of liabilities for intermediaries and the debate for the extent to which they can be held liable. The Information Technology Act, 2000 in India and its amendment in 2008 are the statutes which govern intermediaries in India, Section 79 specifically mentions the intermediary and the due diligence to be taken up by them. Additionally, the Intermediary Guidelines Rules, 2011 also governs the limitations and due diligence of the intermediaries. The Manila Principles of Intermediary Guidelines are available globally. They take into account the Trade and Human Rights aspect of expression. The recent judgements of Shreya Singhal and Baazi.com have also discussed in detail the idea of liability. Further, the liability discussed is not limited to one but has facets like Direct liability, Contributory Liability and Vicarious Liability. The paper also delves into questions of Privacy and Encryption in the light of Intermediary due diligence and the extent of providing access to data. The intermediary liability, therefore, is not just a concept in isolation of cyber jurisprudence but also has facets of freedom and fundamental rights attached to it.

Keywords: Intermediary, Liability, Rights

*#2nd Year Student (BA LLB), Symbiosis law School, NOIDA, Email: ashabaribasuthakur27@gmail.com
1. INTRODUCTION

Intermediary with respect to any records refers to any particular electronic record, any person or any entity which on behalf of any other person stores, receives and transmits the record of information or provides any service with respect to the record is known as an intermediary. Person referred herein could refer to both professional and non-professional intermediaries. Additionally, the intermediary could also provide service which is referred to as “value added service”. This could include formatting, translating, recording, authenticating, certifying, preserving data messages and providing security for electronic transaction.2 The use of internet in the recent years has increased in the personal arena and business fields. The intermediary liability hugely impacts the growth and development of internet. They have become units of control in the cyberspace. This includes natural persons, non-commercial users and business users. 3 The intermediary liability has increased with the operation of cybercriminals.

1.2 DEFINITION OF INTERMEDIARY

Intermediaries are entities that provide services enabling the delivery of online content to the end user.4 Intermediary is defined in Section 2(1)(w) of the Information Technology Act, 2000. The liability is described in Section 79 of the Act. The intermediaries are bound by the Intermediaries Guidelines Rules, 2011.

2. EVOLUTION OF INTERMEDIARY LIABILITY

The concept of intermediary has surfaced due to the distinctive architecture of the internet.5 The internet is known as the hub of information. This process is facilitated by intermediaries. Vast amounts of data and information are transmitted across borders in seconds. The internet as a field lacks jurisdiction and the lack of tracing of data causes anonymity to the various cybercrimes.

2 Bhansali, Commentary on the Inf
5 Pritika Rai Advani, “Intermediary Liability in India”, Economic and Political Weekly, Vol. 48, No. 50 pp. 120-128, (December 14, 2013),
2.1 MANILA PRINCIPLES ON INTERMEDIARY LIABILITY

The intermediaries over the internet have facilitated the internet for all the other consumers. Therefore, the liability of the intermediaries also affects the users of the internet. This includes the right to freedom of expression, freedom of association and the right to privacy. The Manila Principles are six principles to guide the government, industry and civil society for the regulation of the content of the intermediaries.\textsuperscript{6}

The Manila Principles were inspired by the International Principles on the Application of Human Rights to Communication Surveillance. The aim was to maintain limits which were proportionate to the liability of the intermediary. This was taking into account the borderless nature of the internet and the effect intermediaries have in their reach globally.

The drafting of the Principles take into consideration certain legal backgrounds of legislations and the effect the law would have.

The Human Rights Law construct the Freedom of Expression. It is not only the fundamental in the Indian Constitution but also is enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights.

The Trade and Competition context, the compliance cost of companies is taken into account. An uniform approach of law is sought for to enable a clear legal framework. Since the internet is not limited by jurisdiction, a cross border approach would be beneficial for not only the local trading corporations but also foreign companies.

The Principles enshrined in the Manila Intermediary Liability are:

I. Intermediaries should be shielded by law from liability for third-party content.
II. Orders and requests for the restriction of content must be clear and unambiguous.
III. Content restriction policies and practices must be procedurally fair.
IV. The extent of content restriction must be minimized.
V. Transparency and accountability must be built in to content restriction practices
VI. The development of intermediary liability policies must be participatory and inclusive

The Section 79 of the IT Act has been based on the lines of the Manila Principles.

2.2 SECTION 79 OF THE IT ACT

Section 79 of the IT Act discusses the due diligence of such intermediaries. The intermediary shall not be liable for any third party information hosted by it, if its function is limited to providing access to a communication system over which information of the third parties is transmitted or temporarily stored or hosted or the intermediary is not liable for initiating transmission and rightly observes the guidelines of due diligence. This is known as the safe harbour protection. Although, initially the protection provided under the IT Act was limited, after the IT (Amendment) Act, 2008, the ambit of the safe harbour responsibility of the intermediaries has widened. Previously, such protection from liability was provided to only “Network Service Providers”. Moreover, the defence applied only to the offences that had been committed under the IT Act and not to offenses committed under the other laws. In the Bazee case, Mr. Avnish Bajaj was charged under Sections of 292, 294 and 439 of the Indian Penal Code and S.67 of the IT Act. Therefore, the protection provided by the intermediary was inadequate in that context.

In the Amendment Act, 2008, the Intermediary has been given with a revised definition. The objective has been to create greater protection to the intermediary. All service providers have also been identified as intermediaries. The provision is now more transparent since the exemption from liability for any unlawful content/information using an intermediary’s infrastructure is clearly stated. The intermediary needs to maintain compliance under the IT Act. It needs to adhere with the Central Government guidelines under S.67 C for preservation and retention of information.

Safe harbour Protection is a provision which affords protection from liability or penalty. The rationale for providing internet intermediaries safe harbour is that, given the obvious technical and economic impracticalities, intermediaries cannot be expected to monitor content and material circulated in its website.

10 Black’s Law Dictionary
11 Apar Gupta, Commentary on Information Technology Act : with rules, regulations, orders, guidelines, and reports, (Lexis Nexis, Nagpur, 2nd edn., 2011) [hereinafter Apar].
The Shreya Singhal\textsuperscript{12} judgement is of particular relevance in this context. The court upheld the validity of the section but with a few alterations. If the intermediary receives the “actual knowledge” of any content posted on its website, it is bound to remove it within the next thirty-six hours. If it fails to observe the same, it shall lose its immunity and can be sued for offensive and defamatory content.\textsuperscript{13} In the judgement the nature of “actual knowledge” was changed. Formerly, the request to take down any offensive information could come from the Government, the Court or any public spirited NGO. However, under the scope of the judgement, the knowledge could only be received by the order of the court or any Government sanctioned direction. Upon receiving such an order if the intermediary fails to remove the offensive material within the next 36 hours, then it would be liable to be sued.

3. MISCONDUCT

The internet and its wide pool of information have benefitted people in a lot of ways. Although, traditional method of viewing intermediaries would be to exempt intermediaries from wrongful conduct as they are not the active part of the wrongful act. According to this approach, those who use the services should be regulated directly.\textsuperscript{14} However, it is often observed that internet intermediaries need to be regulated as well. They play critical roles. The recent amendments and drafts focus on the limitation of the freedom of intermediaries. The recently drafted, Information Technology (Intermediaries guidelines) Rules, 2011 provide for the due diligence and the limitations on the intermediary benefits.

3.1 THE END-TO-END ENCRYPTION OF THE INTERNET

The Rules notified by the Ministry of Electronics and Information Technology (MeitY) on December 28, 2018 demanded greater diligence from intermediaries. These include:

It has been presented that there should be technology based controls so that there is removal and disabling of unlawful information or content based on automated methods. This has,

\textsuperscript{12} (2015) 5 SCC 1.

\textsuperscript{13} Apar Supra note 10.

\textsuperscript{14} Apar Supra note 10.
however, been argued against by Open-source companies\(^\text{15}\) like Wikepedia and Mozilla. Their argument rests that it is not possible to monitor all content available due to their open source.

Due to increase in cyber-crime, establishing the source of content is required. This could lead to the choice of dismantling the system of end-to-end encryption or restriction from the use of intermediary liability. This has created issues for networks like Whatsapp, Facebook, etc, whose core values stand upon protecting user data. Such guidelines could make it impossible for such applications to function in India. Therefore, Encryption works adversely as well as for the data protection. Infiltration into such encrypted data would lead to violation of the Right to Privacy. Therefore, tougher scanning mechanisms need to be developed by these organizations by themselves and take up steps to minimize cyber offences.

3.2 THE GATEKEEPER LIABILITY

The idea of the Gatekeeper Liability surfaced in the two papers written by Reinier Kraakman in the 1980’s.\(^\text{16}\) The approach is not a normative one taking into account the level of responsibility, participation or support of the intermediary; rather, it is the balancing approach about misconduct and intermediary sanction in the misconduct. The object of the approach is that the intermediary should act as a gatekeeper, It should not only detect offenses but also be able to prevent offenses. Therefore, to be a sufficiently capable intermediary, it should have a sufficiently large market structure to prevent any illicit activity on the internet. Plausibly such dominant powers would help minimize the unlawful activities on the internet. Payment intermediaries like Visa and Mastercard are relevant examples of gatekeeper intermediaries.

The question of gatekeeper intermediary and misconduct has been a traditional question. The role of the intermediary in adhering damages to the primary misfeasors has been debated. The question has been whether the liability should be strict or based on negligence or fault.


Tort based liability would impose greater risk on the intermediary as it would leave the intermediary exposed to damage if it fails to adopt adequate steps to detect and control misconduct.

More recent approaches talk about advances in technology and how it would be useful in to monitor networks effectively. They also talk about cheaper monitoring networks to eradicate activity that is not desirable. The liability of the Primary misfeasors has been increased while the intermediary needs to observe due diligence. There is observed a trend of reluctance for applying strict liability to the intermediaries. In Religious Technology Center v. Netcom On-Line Communications Services, Inc.\textsuperscript{17} the court stated that it does not make sense to adopt a rule of strict liability which would lead to a party being liable whose liability is merely restricted to the creation of operation on the internet. Holding of the strict liability standard would hold the entire internet liable without any fault of its own.\textsuperscript{18} Therefore, holding the intermediary liable would be unpragmatic.


The Information Technology (Intermediaries guidelines) Rules, 2011, originally the due diligence observed by Intermediaries Guidelines (Draft) Rules, 2011 was notified on April 11, 2011. The Rules had been drafted to assist internet intermediaries to avail the exemptions under S.79 of the IT Act. Pendency of the cases against the online service providers was one of the reasons for the amendment of the Section and the introduction of the Rules. The case of Bazee.com\textsuperscript{19} further demanded clarity on rules of exemption for the intermediaries.

Further, the guidelines for the observance of due diligence and notification are provided in the Intermediary Rules. An argument is that this will lead to reduction in freedom of speech and expression. The possible problems to be faced are:

Firstly, the classifications of content which can be removed are excessively broad. There are no specific legal standards established in the civil and criminal codes for adhering of liability. The Rules create “content code” for the Internet.

\textsuperscript{17} Ibid.


Secondly, in the absence of any well-defined legal standards, the private censorship is of particular relevance. This is different from other codes, where the Government imposes restrictions after balancing the interests and good of the society. There are separate statutes for the same under every civil and criminal law; however, it is left to private interests in case of the IT Law. Moreover, there are safeguards for appeal for each of such cases. Hence, it is necessary that the competing interests are finely balanced by courts even in the Information Technology Legislation.

Thirdly, under this law, the intermediary is treated as a corporate entity. The entire objective of the corporate entity is to foster such practice and undertake such responsibility so that it does not lose the protection conferred to it.

An important illustration of the same is the case of TATA v. Greenpeace Case. The litigation was asked to remove content on the grounds that it was defamatory and causing infringement on the TATA trademark. Therefore, a civil suit would also be sufficient to proceed under the rules.

3.4 Intermediary Liability To Preserve Data And Provide Technical Assistance.

As per Central Government Guidelines, an Intermediary is required to preserve and retain information under S. 67 C of the IT Act, 2000. Under S. 69B it also needs to offer technical assistance to authorized agencies for the transmitting, receiving and storing of data. Failure to comply with such terms could lead to punishment of imprisonment and fine. Under S. 70B (7) of the IT Act, with regard to the protection of the Critical Infrastructure, the intermediaries are required to provide information to the Indian Computer Emergency Response Team. Failure to comply with the same could also result in punishment.

4. Liability

The Liability of the intermediary can be of three types: Direct, Contributory or Vicarious.

---


4.1 **DIRECT LIABILITY**

In order to make an intermediary directly liable, some acts apart from hosting is required. If the intermediary had previous knowledge of the Act being committed, it shall be guilty of Contributory infringement. Substantial or material contribution is essential for inducing direct liability. Therefore, if infringement is carried out directly then the infringement is direct infringement. If there is abetment or inducement, then the infringement is contributory. This was also held in the Netcom case\(^\text{22}\) that in order to hold an intermediary liable, some additional acts on behalf of the intermediary apart from mere hosting of the data is required. In case there is no verification of the infringement in case of the alleged act done, the intermediary would not be held liable.

4.2 **CONTRIBUTORY LIABILITY**

The concept of Contributory Liability is provided in S. 79 (3)(a) of the IT Act, 2000. It says that the intermediary would not be let off of liability if it had conspired, abetted or aided or induced by promise, threat or by any other action, the Intermediary shall be held liable. The intermediary herein mentioned should have the knowledge of the illegal activity it would have caused and the nature of harm so caused due to such infringement or inducement.\(^\text{23}\) The intermediary can also be held liable for contributory negligence when despite the notice of having the knowledge of material being unlawful; the intermediary does not do any act regarding the same and does not delete it despite notice. If an intermediary keeps infringing material at a low price on the website\(^\text{24}\), or maintains control over process to copy infringing materials\(^\text{25}\) or provides network/software to commit infringement\(^\text{26}\) or promote users to upload infringing materials\(^\text{27}\) or advertises it extensively\(^\text{28}\), trend or history of infringements\(^\text{29}\) or category of goods as subject matter\(^\text{30}\) contributory liability would lie.

\(^{23}\) Karnika Supra note at 20.
\(^{26}\) A & M Records Inc. v. General Audio Video Cassettes., Inc.m 948 F. Supp 1449 (C.D. Cal 1996).
\(^{28}\) Columbia Pictures Indus Inc v. Russ Hardenburgh Inc., 982 F, Supp 503, 514
\(^{30}\) Recording Industry Association of America Inc. v. Diamond Multimedia System Inc., 180 F 3d 1072 (9th Cir 1999)
4.3 Vicarious Liability

The traditional concept of vicarious liability requires the defendant and the infringer have an association of employment or partnership, that invokes the concept of enterprise liability on master if the employee negligently performs his duties as his acts blinds the master in transactions as regards to third parties.\(^{31}\) It is based on the principles of *respondeat superior*. Under enterprise liability, the defendant is held liable for the Acts committed by any other person.\(^ {32}\) Vicarious liability is enforced even if the entity is unaware of the infringing activities. The defendant should possess the right and the ability to supervise the infringing conduct and there should be financial interests involved.

In *Playboy Enterprises, Inc. v. Frena*\(^ {33}\) the court found the defendant board vicariously liable for the unauthorized images that were uploaded in the magazine of the plaintiff.

5. ANALYSIS OF CASES

5.1 Bazee.com Case\(^ {34}\)

**Facts:** Bazee.com India Private Limited was a platform for online market where buyer and seller could interact for the purpose of transaction. On the platform, a seller had placed an MMS clip for sale. The buyer interested could get a copy of the clip after payment. It was soon circulated that the platform was selling clips that were illegal and were under the ambit of pornography. The video clip was ultimately removed. However, it had been already sold to various people all over the country. The seller of the video clip as well as the CEO and the Director were arrested.

**Laws:** Section 79 IT Act, Section 85 of IT Act.

**Analysis:** The Court observed that the Director and CEO of Baazi.com could neither prove that he did not have knowledge nor could he show that he had observed due diligence as an intermediary towards the third party. The liability herein was vicarious in nature.

---

\(^ {31}\) Karnika *Supra* note at 20.

\(^ {32}\) Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability*


\(^ {34}\) (2005) 3 CompLJ 364 Del.
Section 85 of the IT Act provides the liability of the Director vicariously when such acts are committed and a charge of contravention is made. Therefore, the FIR of the director could not be quashed. However, the Court held that there could be no mens rea proved against the director. Therefore, there was no implied and automatic liability on him. Section 85 further provides that when offence is created by any company, every person who at that time was responsible for the business at that point of time was liable to receive punishment unless lack of knowledge or observance of due diligence is proved. If there is perious consent of the Director, he shall be held liable.

Due to the absence of due diligence mechanisms, there was no safe harbour protection or exclusions for third party content transmissions, the FIR continued. The internal filters failed to block the obscene MMS clip that was uploaded.

After the amendment of Section 79 of the IT Act, there has been greater clarity about the liability of the intermediary. The intermediary is not liable if it undertake due diligence or if it does not have actual knowledge about any content that is published on its platform.

5.2 Sanjay Kumar Kedia v. Narcotics Control Bureau

Facts: The appellant Sanjay Kumar Kedia owned tow companies M/s Xponse Technologies Limited and M/s Xponse IT Services Pvt. Ltd. A search was conducted at the premises of the appellant. Although nothing incriminating was found, he was issued notice by the NCB. Thereafter, bail applications were filed by the appellant. They were accused of hosting pharmaceutical websites and using huge amount of psychotropic substances on these websites. Therefore, not functioning merely as an intermediary but also engaging in sinister activities.

Laws: S. 79 of the IT Act.

Analysis: The Petitioner’s plea for seeking of immunity under the purview of being an intermediary under S.79 of the IT Act was declined. The Petitioner had knowledge of the mala fide actions and marketing of Xpose Technologies Ltd. and Xpose It Services Pvt. Ltd. They were marketing the substances to the US and other countries causing violation of the NDPS Act. Hence, They were not liable to be granted the status of the immunity under the IT Act, 2000.

In 2011, the issue of pre-censoring of the third party information which had been posted on the internet gained limelight.\textsuperscript{36} Like other cyber laws in the country, the intermediary laws are also going through immense changes and in an attempt to understand the scope of the legislations. Due to the nature of the internet and the globalization which affects it, such legislations cannot work in isolation. Therefore, the liability in the country is also drafted according to the global framework of the intermediaries. There has been shift from the traditional approach and the IT laws are often related in the purview of freedoms and other trade related laws. Further, the IT (Intermediary Guidelines) Rules, 2011 also determine the content of the intermediaries. Illegal content posted by any user needs to be removed within 36 hours of complaint by an aggrieved person on various grounds.

The due-diligence to be observed by countries also would vary according to jurisdictions. If Government proposes to pre-censor third party content, the ambit and scope of such regulation and the technical feasibility is to be considered. The liability of the intermediary as well as the IT Act is to be clarified from the Indian Penal Code, 1860. The clarity in the legislation will come from the Parliament or the Judicial decisions. For instance, on consumer blogs complaining about deficient services of a service provider is protected by free speech so long as it does not use abusive language or becomes defamatory.\textsuperscript{37} Therefore, there needs to be better development of netiquette so that the users of the internet are able to distinguish their freedoms and rights, especially their free speech and expression and become more aware citizens of the internet world.

5. CONCLUSION

The Indian Laws, though resembling the global framework of laws on a remote level, lacks detail. Although the amendment in the Act and the Intermediary Guidelines have expressed concerns about the safe harbour and due diligence, the threat to Right to Freedom of Speech and Expression need to be addressed. There should be more clarity on jurisdiction with the principles of immunity. The trade laws and constitutional laws should be balanced in determining this approach. The aim of the judicial decisions should be to decrease the burden on intermediaries and allow them greater ease of work. Thus, the present law in India must be

\textsuperscript{36} Karnika \textit{Supra} note at 20.

\textsuperscript{37} Karnika \textit{Supra} note at 20.
carefully developed by both the legislature and judiciary to create a clear, comprehensive and fair framework with regard to intermediary liability.

6. SUGGESTIONS

In the light of the above research, we want to recommend the following suggestions:

(i) **Drafting of Ancillary Legislations:** Most of the Legislations till date have ignored the freedom of speech and expression. The same needs to be considered.

(ii) **Freedom of Intermediaries through Judicial Pronouncements:** To substantiate the legislation, judiciary should create more ease to the intermediaries.

(iii) **Jurisdiction:** Adopting better methods of determining Jurisdiction on the internet. This would facilitate the intermediaries in providing better access.