Intermediary Liability and Child Pornography: A Comparative Analysis*

Anjali Anchayil & **Arun Mattamana**
II Year, B.A. L.L.B. (Hons.)
National Law School of India University, Bangalore, Karnataka, India
Email: arunbmattamana@gmail.com
anjalianchayil@gmail.com

Abstract. With the increasing instances of transmission of child pornography over the internet, the liability of the host of service providers who facilitate the transmission of the content has become a contentious issue. With varying legal regimes, jurisdictional issues and standards of obscenity applied as well as varying degrees of care to be exercised, this area is a legal quagmire. This article addresses the question of whether we need an intermediary liability regime or not. The article posits that intermediary liability does not address the question of preventing transmission of child pornography as the actual culprits remain beyond the reach of law. A scheme of intermediary liability only acts as a disincentive to the intermediary to innovate and hinders growth of internet services. A comparison of three regimes, United States, European Union and India, is undertaken to see the legislative measures, developments in case law and analyze their stand towards the intermediary. The Article finally works towards arriving at alternative options so that the autonomy of the intermediary is not compromised through over-regulation and censorship.

I. Internet and Intermediaries

Internet activity is composed of packets of data, which are sent over privately owned networks.[1] However this service has to be provided by a group of service providers known as intermediaries. They consist of service providers, web hosting companies, bulletin board operators, search engines etc. which facilitate and process hundreds of millions of data transfers every day and host or link to literally billions of items of third party content.[2]

Intermediaries are defined by the Information Technology(Amendment) Act, 2008 of India as "*with respect to any particular electronic records, 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.*"[3]

The intermediaries can be classified into various groups according to the functions they perform, which include communication gateway providers, permanent data hosts, transitory data hosts and linking intermediaries. Permanent hosts provide a permanent storage for the uploaded files while the transitory data hosts provide temporary storage. At the same time linking intermediaries provide a platform for hyperlinks that lead to other locations on the net.

The role and liabilities of intermediaries has been under the scanner in recent times due to the development of the internet in ways that had probably not been imagined by the inventors of the Web. The anonymity and ease of access provided by the internet has resulted in pedophiles making it their modus operandi to lure children. Chat rooms, bulletin boards, discussion groups, social networking sites etc have been used as platforms for spread of child pornography. In such situations, the question of who should be held responsible for the criminal activity becomes important. Intermediaries seemed a viable option as they have the ability to regulate the content online at very minimal costs. The main debate in this regard has been about the nature of liability to be imposed on them. Should a strict liability regime be enforced or a fault based liability regime?[4] With a strict liability system, an ISP will be held liable regardless of its knowledge and control over the material that is disseminated through its

* This paper was originally published in Kierkegaard, S. (2009) Legal Discourse in Cyberlaw and Trade .IAITL.
[1] Apar Gupta, *Liability of Intermediaires in India: From Troubled Waters to Safe Harbours*, C.T.L.R. 2007, 13(2), Rev. 60,61 (2007).
[2] Mark A. Lemley, *Rationalizing Internet Safe harbours*, 6 J. Telecomm. & High Tech. L. Rev. 101, 102 (2007).
[3] Information Technology Act, Section 2 (2008) (In.)
[4] Pablo Asbo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce, At* http://www.chtlj.org/sites/default/files/media/articles/v019/v019.i1.Baistrocchi.pdf

facilities. In a system based on fault,[5] an ISP would be held responsible only if it intentionally violates the rights of others[6] or takes part or permits the trade after having knowledge of the content itself.

This article makes an argument against the imposition of intermediary liability in instances of child pornography through a comparison of legislations and developments in case law in three regimes. A comparative analysis of the systems in the United States and the European Union countries, as against India, a developing country, has been employed to evolve an ideal regime. This caters to the objective of prevention of child pornography while promoting development of better and more interactive Internet services. The second section deals with the approach taken by the United States against child pornography by evaluating the legislative measures and the stand taken by the judiciary in interpreting them. It also deals with the European Union's approach and the national legislations enacted to conform to it. The section additionally looks into how a developing country like India has included provisions dealing with cyber pornography along with facilitating growth of Internet services. The last section proposes alternative options to imposition of intermediary liability.

2. Comparative Analysis

2.1 United States of America

The United States has the infamous reputation of being the largest market for child pornography.[7] With the coming of the Internet, its transmission has become easier, faster and secure. Large scale sale and dissemination of pornographic material takes place online through chat rooms, discussion groups, bulletin boards, websites etc. Concerns about the exposure of children to child pornography, child sexual tourism, pedophilia etc has led the US to enact a number of federal as well as state legislations to combat the menace of pornography online. This section deals with the position of intermediaries in the US and how far liability has been attached to them in the laws enacted to combat pornography.

Miller v. *California* [8] laid down a three-point test for obscenity. The standards laid down in this are as follows i) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest ii) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law iii) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value. The *Miller* test has stood the test of time for more than a quarter-century. The applicability of the Miller test to the Internet is debatable, as (which?) immunity standards have to be applied is unclear in the definition.[9] Is it the standards applicable in the jurisdiction from which the purveyors send the material or the standards applicable in the receiver's country? These issues have largely been settled by the courts using expert testimony from various individuals in diverse fields, community polls, etc., [10] with the effect that the Miller test still remains the conclusive test for obscenity till date. It was also held in *Ashcroft* v. *American Civil Liberties Union*[11] that for the purpose of the Child Online Protection Act which prohibited commercial display of sexually explicit materials harmful to minors on the Web, community standards do not have to be defined with reference to a particular jurisdiction or geographical area, which was found to be a fundamental flaw in the *Miller* test.

The question of intermediary liability evolved with time as the legislative framework developed to include regulation of the Internet. The US enacted the Child Pornography Prevention Act in 1996, which defined child pornography broadly so as to include computer-generated images of children also. Though the Child Pornography Prevention Act sought to prosecute pedophiles, it did not say anything about the prevention of exchange of pornographic materials over the Internet and as such did not apply to intermediaries.[12]

The courts initially employed the theories of direct liability whereby the online intermediary was held liable for the subscriber's behaviour, contributory liability if the ISP having knowledge of the infringing activity induced, caused or materially contributed to the user's infringing activity or vicarious liability if the ISP had the right and ability to monitor the actions of the subscribers, neglecting to do so and profited from the infringing

[5] Public Prosecutor v Neij, Unreported April 17, 2009.
[6] *Supra* note 4
[7] George Ivezaj, *Child Pornography on the Internet: An Examination of the International Communities Proposed Solution to the Global Problem*, 8 MSU-DCL J. Int'l L. Rev. 819,819 (1999).
[8] *Miller* v. *California*, 413 U.S. 15 (1973).
[9] Karl A. Menninger, *Cyberporn: Transmission of Images By Computer As Obscene, Harmful to Minors or Child Pornography*, 61 Am. Jur. Proof of Facts 3d 51. Rev. §1, §5 (2009).
[10] *Id.*
[11] *Ashcroft* v. *American Civil Liberties Union*, 535 U.S. 564.
[12] *Supra* note 7

activity.[13] The Digital Millennium Copyright Act and the Communications Decency Act were enacted which brought in a certain degree of immunity to the ISPs as it recognised the perils of such regulations as stifling growth, slowing innovation and (as involving) too much censorship.

The question of regulation of content online has always been subject to much debate due to the conflict with freedom of speech guaranteed by the First Amendment. Obscenity is out of the purview of protection given by the First Amendment. However, courts in the US have always applied a strict scrutiny test to statutes abridging speech excluded from protection by the First Amendment.[14]

The privilege created by section 230(c)(1) of the Communications Decency Act (hereinafter referred to as CDA), 1996 has guaranteed free speech on the Net by giving immunity to the provider or user of an interactive computer service for the information flowing through their networks.[15] The CDA encourages voluntary action on the part of ISPs by granting them immunity if they take measures to restrict access or availability of material that the provider considers to be obscene in content.[16]

In *Zeran* v. *America Online*[17], the court denied a claim against AOL on the basis of distributor liability. In the suit for negligent dissemination of information, AOL pleaded immunity under section 230(c) of CDA. The court expanded the immunity provision so as to give protection to ISPs from suits based on both publisher and distributor liability. Treating AOL as a distributor of the information and subjecting it to the knowledge or reason-to-know standard would be equivalent to considering it as a 'publisher or speaker' of third-party information. Therefore, the court held that distributors are 'publishers' encompassed by the immunity provision.[18] This case where it was held that section 230(c) "*creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service*," irrespective of whether the ISP was acting in the capacity of a publisher, distributor or both has broadened the scope of immunity granted, ISPs have escaped liability in most cases including pornography which is not granted protection under the First Amendment through the immunity granted by Section 230(c) of the CDA. Through judicial interpretation, courts have taken the trend away from ISP liability thus pre-empting state laws which would otherwise have required the ISPs to take due care.[19]

The case *Doe* v. *America Online*[20] is illustrative of how section 230 interpretations have resulted in a favourable ruling for AOL in a case of child pornography. AOL was not held liable for not monitoring the chat room thereby violating obscenity statutes. In *Doe* v. *GTE Corporation*,[21] a case involving athletes who were secretly filmed while undressing, the ISPs were sued by the athletes. However, the court did not attach any liability to the ISP. Easterbrook, J. said in this case that ISPs were analogous to common carriers which were not liable for the dangerous material they might transport and telephone companies which were not liable even if the telephone had been put to use for illegal activities. The position of an ISP was similar and he found no reason why they should be not be absolved of liability.

Section 230 has been interpreted broadly so as to create absolute immunity for any ISP even if they had knowledge of the unlawful nature of the content and failed or refused to remove it.[22] A look into the development of case law will elucidate this point. *Zeran*'s reasoning was followed in *Drudge* v. *Blumenthal*[23] where the court said that '*[i]n some sort of tacit quid pro quo arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.*' [24] The court thereby illustrated the growing trend towards absolute immunity for intermediaries. In *Doe* v. *MySpace*,[25] a case involving sexual harassment of a child by a MySpace user whom she met online, the mother brought an action against MySpace for not having provided adequate safety measures to prevent child sexual harassment. The Court used the logic in *Zeran* saying that the plaintiffs were attempting to hold MySpace liable as a publisher. The court noted that the CDA immunizes ISPs for "ineffective security measures" so as to incentivize ISPs to self-police without risk of more liability for doing so. The Court also held that without the immunity granted by the

---

[13] Luca Tiberi & Michele Zamboni, *Liability of Service Providers*, C.T.L.R., 9(2). Rev. 49, 52 (2003).
[14] Farzad Damania, *The Internet: Equalizer of Freedom of Speech? A Discussion on Freedom of Speech on the Internet in the United States and India*, 12 Ind. Int'l & Comp. L. Rev. 243, 249 (2002).
[15] Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 Pepp. L. Rev. 427, 433 (2009).
[16] 47 U.S.C. § 230 (c) (2) (A).
[17] *Zeran v America Online*, 129 F3d 327 (4th Cir 1997)
[18] Susan Freiwald, *Comparitive Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 Harv. J.L. & Tech. Rev.569, 638 (2001).
[19] Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 28. 14 Sup. Ct. Econ. Rev. 221, 223 (2006).
[20] *Doe* v. *America Online*, 718 So 2d 385 (4th Cir., 1999).
[21] *Doe v. GTE Corp*., 347 F.3d 655 (7th Cir. 2003).
[22] *Supra* note 2 at 103.
[23] *Blumenthal v. Drudge*, 186 F.R.D. 240-42
[24] *Supra* note 19 at 642.
[25] *Doe v. MySpace*, Inc., 474 F.Supp.2d 843 (WD Tex. 2007).

CDA, MySpace and similar sites would choose to indulge in a policy of restricting the number and type of messages allowed to be posted, which would only frustrate Congress' goal of encouraging such interactive computer services to create forums for citizens to exchange their thoughts and ideas. Also, if liability was imposed after even after putting a security regime in place, the court felt that ISPs would not implement such measures at all.[26]

Even the knowledge standard has been given a go-by as illustrated by the case of *Doe* v. *Bates*[27] in which the plaintiff sued Yahoo! for displaying images of pornography which had been put up by him even after he was arrested. His argument was that Yahoo should be liable as it profited from the illegal activity as it had been receiving revenue from advertisements placed on the group. Yahoo! argued that knowledge was irrelevant to immunity under Section 230 of CDA. The court applied *Zeran*'s reasoning concerning defamation to the issue of child pornography and held that if Yahoo! were to be liable for deciding what content to be permitted, it would have not have any incentive to regulate at all. The sheer number of postings would make monitoring impossible. The court's concern was that, without immunity, Yahoo! and other such services would censor too much legal speech so as avoid exposure to litigation. The court called this over-censorship of speech the 'chilling effect.'[28] Similar was the case *Ramey* v. *Darkside Productions*[29] where the website was not held liable for sexually explicit photographs even though it had actual knowledge that the photographs violated the intellectual property rights. Immunity under Section 230(c) was given to the site.

The CDA was struck down in *Reno* v. *American Civil Liberties Union*[30] where the court held the statute to be broad in as much as the provisions restricted the constitutionally guaranteed speech to adults by not defining "indecent" and "patently offensive." The defences provided to the ISPs, such as, the defendant having taken appropriate measures to prevent access to such content to minors and restricted access by requiring credit card, debit card, adult access code or adult personal identification number, was considered not to be available to many users. As a consequence, the US Congress passed the Child Online Protection Act of 1998 which prohibited anyone from making any communication for commercial purposes on the Internet that contained material harmful to minors.[31]

The Child Online Protection Act was struck down by the court which held that the Act was not narrowly tailored to meet the compelling state interest in restricting material harmful to minors and that it violated freedom of speech under the First Amendment as it restricted speech which was not prohibited for adults. The court also held that use of filtering technology would be a more efficacious remedy for sexually explicit material rather than the COPA.[32] In *American Civil Liberties Union* v. *Ashcroft*,[33] the court held that the COPA definitions imposed too great a burden on Web publishers even if they did not profit from the material or post such material as part of their business.

The approach of the US has been pro-ISPs as courts and the legislators have largely concluded that if intermediaries were to be held liable every time objectionable content has been posted online, the threat of liability and efforts at clearance could weaken the Internet.[34] There has also been an increasing tendency against imposing criminal prohibitions against ISPs as even though the state had an interest in preventing child pornography, there were better options such as filtering systems, child friendly software etc.[35]

2.2 European Union

The European Union's E-commerce Directive was an ambitious project introduced in the year 2000. The Directive was formulated for providing proper guidelines to the internet intermediaries and their liabilities. The Directive defines what an intermediary[36] is, and also states that the intermediaries are not liable unless if in the transmission of signals, they had any role in initiating, selecting the receiver or modifying the information. This measure was intended as a safe harbour to the intermediaries. However, the provisions laid down in the Directive have not been

[26] Zac Locke, *Asking For It: A Grokster Based Approach to Internet Sites That Distribute Offensive Content*, 18 Seton Hall J. Sports & Ent. L. Rev. 151, 173 (2008).
[27] *Doe v. Bates*, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006).
[28] *Supra* note 26at 174.
[29] *Ramey* v. *Darkside Productions*, 2004 U.S. Dist. LEXIS 10107 (D.D.C. May 17, 2004).
[30] *Reno* v. *American Civil Liberties Union*, 117 S. Ct. 2329.
[31] *Supra* note 9at §13.
[32] *American Civil Liberties Union v. Mukasey*, 534 F.3d 181.
[33] *American Civil Liberties Union* v. *Ashcroft*, 322 F.3d 240 (3d Cir. 2003).
[34] *Supra* note 2.
[35] *Cyberspace Communications, Inc. v. Engler*, 142 F. Supp. 2d 827 (E.D. Mich. 2001).
[36] Michael J Coyle, *Liability of Intermediary Service Provider*, Lawdit Reading Room, *at* http://www.lawdit.co.uk/reading_room/room/view_article.asp?name=../articles/Liability%20of%20intermediary%20service%20providers.htm

entirely implemented in the national legislations of various countries such as Sweden and hence many of them do not protect internet intermediaries from unreasonable liability.[37]

Cases of paedophilia in the European region have resulted in a stricter approach towards child pornography. The Dutch police busted a child pornography ring and also the case of Belgian police attempting to identify 350 children in captured DVDs and cassettes.[38] The scenario of increasing cases of child pornography online resulted in a call for cooperation between the internet intermediaries and the governments. Recognising the legal uncertainty caused by issues of jurisdiction regarding cross-border activities, the European Commission developed a harmonized set of rules to limit the liability of some Internet Service Providers (ISPs). Article 12 of the E-Commerce Directive deals with the 'mere conduit' function and limits the civil and criminal liability of service providers that merely act as conduits of data, which means that this exemption applies to service providers that transmit information from one point on a network to another, at the request of the recipient of the service or that simply provide access to a communication network without being in any way involved in the information transmitted. Thus the Directive sets up guidelines which follow a system of with-fault liability than an unreasonable strict liability. The European Commission adopted the new rules on June 8, 2000, as part of the E-Commerce Directive. Nine years after the adoption of the Directive, national case law across Europe has been evidencing a trend imposing a greater responsibility on the ISPs.[39]

The United Kingdom has followed stringent measures fixing intermediary liability in the case of child pornography. Under the Protection of Children Act, 1978, it is a criminal offence to "take, *distribute, exhibit, or possess even one 'indecent' photograph of a child"* in England and in Wales. The PCA was amended by the Public Order Act to include data stored on a computer disc or by other electronic means which is capable of conversion into a photograph. It criminalized morphed pornography, which was defined in the act as '*an image, whether made by computer-graphics or otherwise, which appears to be a photograph.*' The Sexual Offences (Conspiracy and Incitement) Act of 1996, made putting child pornography on the internet punishable in the U.K. It also bans underage sex incited using the internet in the United Kingdom and Wales. The state also notified the internet intermediary about what content is illegal and what is not in a move to encourage ISPs to regulate them.[40] However unlike the US, the punishment for possession of pornographic material is quite low as the imprisonment awarded in these cases is fixed at six months only.[41]

The UK government has also set up the Internet Watch Foundation to regulate child pornography. This independent organization provides a mechanism of a hotline which enables individuals who come across illegal content on the web to give due notification to the police. It is seen that the relationship between internet intermediaries and the government is free from much cumbersome obstacles. While the Parliament passes the laws, the industry helps carry them out, through the co-operation of the public and the police. However, the minimal prison sentences do not always serve as an effective deterrent for paedophiles.

The E-Commerce Directive was implemented in Germany in various degrees. The German authorities were the first to regulate the internet intermediaries in the European Union. Under the German Information & Communication Services Act of 1997, arose the German Teleservices Act or Teledienstgesetz, the ISPs were obligated to filter out content. However, the case was filed only if it was proved that the internet intermediary got notification of the same and failed to take any action towards it. In the case of *Rolex* v. *Ebay*, it was held by the court that the liability safeguard was only available to civil and criminal liability and not to injunctive claims, and parties can file injunctive suits for the violation of trademark rights.[42] The authorities also introduced CompuServe which allowed users to independently prevent access to undesirable sites.[43] Though the courts have been penalizing intermediaries for dissemination of illegal pornographic content, the country has been thinking of freeing the ISPs from liability while at the same time introducing a task force to check and regulate the content of the sites and its access in the country. The state has developed PERKEO which analyses the content of computers suspected of containing pornographic content.[44] Germany is also leading the campaign for an internet code of conduct[45] to provide international regulation on the materials disseminated over internet.[46]

---

[37] *Supra* note 2 at 113.
[38] *Supra* note 7.
[39] Patrick Van Eecke & Barbara Ooms, *ISP Liability and E-Commerce Directive: A Growing Trend Towards Greater Responsibilities towards ISPs*, 11 NO. 4 J. Internet L. Rev. 3,3 (2007).
[40] Mehagen Doyle, *Bad Apples in Cyber Space: The Sexual Exploitation and Abuse of Children Over the Internet*, 21 Whittier L. Rev. 119, 133 (1999).
[41] Criminal Justice Act, Section 160 (1988). (UK)
[42] *Supra* note 39 at 7.
[43] Ari Staiman, *Shielding Internet Users From Undesirable Content: The Advantages of a PICS Based Rating System*, 20 Fordham Int'l L.J. 866, 892 (1997).
[44] *Supra* note 40.
[45] *Supra* note 40.
[46] *Supra* note 40.

The Pirate Bay case that convicted the owners of the torrent site Pirate Bay[47] established a certain precedent in intermediary liability in Sweden which can be extended to the field of liability for child pornography as well. In this case it was argued that the copyright infringing material was held to be owned by other people and the site only provided links to download the torrents. However, it was held that as the owners of the website made it clear through their message board that their intention was to distribute copyright infringing material they were to be held liable.[48] This can be extended to child pornography in sites and seen if the intention of the website owners or the ISP was dissemination of such kind of materials even if they only provided the links to other sites containing materials analogous to these. Fixing of liability would be determined on the basis of this.

The Netherlands Criminal Code, Article 240(b), Section 1 makes it illegal to manufacture, disseminate, transport, and export pornography involving children under the age of sixteen.[49] Thus the ISPs in Netherlands have a higher obligation as even transportation of illegal material in the site makes them liable.

Belgium has followed an approach of making it mandatory for ISPs to develop regulating mechanisms. Intermediary liability has been done away with to a great extent though. In the SABAM case,[50] it was held that as per the Belgian E-Commerce Act, the ISPs are not liable to monitor the content that is uploaded on their sites; however, the obligation lies on the ISP to develop technology to filter out the content that is uploaded and check it. The court also rejected the argument that the 'mere conduit' clause of the Directive is violated when filtering technology is applied as modification of the content takes place and brings liability upon the ISPs. They held that automatic filtering is just a technical requirement and hence does not violate the clause.[51]

The E-Commerce Directive created a special regime of limited liability that applies to so-called mere conduit, caching, and web hosting providers. It was for developing safeguards for ISPs that dealt with large amount of data and information.[52] However the case law illustrates that the same has not been the policy followed as stringent measures are still imposed by various nations. Resolution of cross border issues with regard to the content provider, user and the intermediary also remains an unsettled issue hindering the effective implementation of legislations intended to prevent child pornography.

2.3 India

The Indian government too has been alive to the threat of proliferation of pornography online and has responded with the enactment of the Information Technology Act, 2000 which specifically addresses the question of obscenity on the net. Internet censorship in India has been quite stringent with manifold attempts to filter the content. These have taken the form of government mandated filtering by asking ISPs to block access to social networking sites like Orkut due to concerns about the content posted on these sites.[53] Instances of journalists being asked to stop updating their Twitter accounts after the Mumbai attack on grounds of security illustrate the level to which internet censorship takes place in India.[54]

Two important questions need to be addressed. First, how far are penal provisions in the Indian Penal Code, 1860 applicable when transactions take place online? What are the standards to be applied in such cases? Second, are stringent measures to be taken against the intermediaries who merely facilitate the transmission of information?

Section 292 of the Indian Penal Code, 1860 does not per se deal with obscenity online. This difficulty was solved by the insertion of Section 29 A which included electronic documents also within the purview of documents thus making the law applicable to electronic media as well. However, the Indian Penal Code was found inadequate to deal with issues of pornography online as fixing liability on the transmitters of information online was found to be difficult as the question of motive or intention was difficult to be proved in their case. Even though section 292 includes overt acts, as well as illegal omissions, section 35 of the IPC puts intention or knowledge to be proved on the part of the party which is quite difficult in the case of ISPs. In *Ranjit D.Udeshi* v. *State of Maharashtra*,[55] the court possibly wishing to dispose of such a technicality of intention being important to prove knowledge of the content has said that the first subsection of Section 292 does not make it necessary for knowledge to be there on part of the offender as in every case if knowledge of the same were to be proved, it

[47] *At* http://www.piratebay.com/
[48] Mikko Manner *et al*, *The Pirate Bay Ruling- When Fun And Games End*, Ent. L.R. Rev. 197, 200 (2009).
[49] Muireann O'Briain, *The International Legal Framework and Current National Legislative and Enforcement Responses*, World Congress Against the Commercial Exploitation of Children 31.4 (1996) *at* http://193.135.156.14/webpub/csechome/2156.htm
[50] *Supra* note 39 at 6.
[51] *Supra* note 39 at 6.
[52] *Supra* note 39 at 8.
[53] Freedom House, *Freedom on the Net 2009-India*, *at* http://www.unhcr.org/refworld/docid/49d4759128.html.
[54] *Id.*
[55] *Ranjit D.Udeshi v. State of Maharashtra,* All Ind. Rep. 881 (S.C. 1965).

would tip the balance in favour of the offender. His liability is therefore strict. However in the case, it was also said that the prosecution had the burden of proving that accused person did intend to sell such an object.

The Information Technology Act, 2000 found a solution to the question of *mens rea* to be proved in case of the IPC as it does not need such a condition to be met while imposing liability.The Information Technology Act, 2000 was introduced to ensure compliance with the resolution of the United Nations for the adoption of United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce.[56] The Provisions of the IT Act together with the ISP guidelines imposed a huge burden on the internet service providers to be on the alert monitoring content that came through their networks.

The instances of assaults perpetrated through the internet have become a cause of concern and has resulted in more and more legislation to curb obscenity on the internet. However what one fears is that the focus has shifted from curbing child pornography on the net to increasing harassment of ISPs through intermediary liability and state regulation. Section 67 of the Information Technology Act, 2000 is the relevant provision dealing with obscenity online which read with Section 2(1) (w) makes a person who receives, stores and transmits a pornographic message liable for the same.[57] Along with this, the ISP guidelines in India in Clause 1.12.4 of the terms and conditions make it mandatory for ISPs to ensure that objectionable, obscene, unauthorised or any other content are not transmitted through his network and to take necessary measures to prevent it.

A strict liability regime, as envisaged by the Information Technology Act, 2000, provided very inadequate safe harbours for the ISPs as they had the burden of proving lack of knowledge and exercise of due diligence to prevent the commission of such an offence.[58] There is lack of clarity as the standards imposed do not specify what standard of knowledge is to be imposed, actual or constructive. What is meant by due diligence also evades definition leading to imposition of an unduly high burden on the intermediary leading them to indulge in excessive monitoring which goes against free speech, privacy of communications online, etc. Irrespective of the role played by the intermediary in the transmission of information, they have always been held criminally liable.

The case *Avnish Bajaj* v. *State*[59] stirred a beehive by bringing to public notice the effect of intermediary strict liability. The case raised many questions regarding the liability of intermediaries for the content that is posted on their site. Are intermediaries who merely provide a platform for potential sellers to sell products to be held strictly liable? Are websites like Google, Orkut etc to be held liable for the comments, blogs etc which users might upload? When an intermediary has a filtering mechanism in place, can it be said not to have exercised due diligence?

In view of the questions raised, the Indian law on pornography online has been amended through the Information Technology (Amendment) Act, 2008 which made substantial amendments to the Act of 2000. The definition given in IT Act, 2000, only included network service providers as intermediaries, thus only immunizing them and leaving out other types of intermediaries giving no immunity to intermediaries like Baazee.[60] The definition of intermediary in Section 2(1) (w) has been expanded to include all sorts of computer services. Such a comprehensive definition ensures that the wide range of intermediaries is protected under safe harbour provisions which were not the case in the Act of 2000.

Germany's Federal Law to Regulate the Conditions for Information and Communications Services ("Multimedia Law"), in Section 5 of Article 1 makes a clear cut distinction between access providers and host providers. Access providers are exempt from any sort of liability for damages though they have a duty to block illegal content if they gain knowledge about it. Host providers on the other hand are liable if they had knowledge of the illegal content and they are technically able to block the content. The Indian law so far does not make any sort of distinction between the intermediaries involved and applies the same standard to every type of intermediary irrespective of the level of knowledge.

A positive trend has been seen with regard to immunity granted to intermediaries. Section 79 has been modified so as to bring it conformity with the norms adopted by countries of the European Union which regulate liability on the basis of the European Directive on Electronic Commerce 2000.The Directive grants immunity to ISPs when they act as mere conduits and do not initiate the transmission, select the receiver or select or modify the information contained in the transmission. [61] This is a welcome measure as it involves a shift from a strict liability perspective to a with-fault liability rule where the intermediary is held liable only if he had knowledge of the transmission.

The stand on pornography continues to be that of dealing with intermediaries with an iron hand. The section on obscenity has been expanded to include a specific section on child pornography as an exclusion from

---

[56] Shalini Agarwal and Satyendra Shrivastava, *Brief Overview of Internet and E-Commerce in India,* C.T.L.R. 13(7). Rev. 212, 212 (2007).
[57] Information Technology Act, Section 2(1)(w) and Section 67 (2000) (In.).
[58] Information Technology Act, Section 67 (2000) (In.).
[59] *Avnish Bajaj v. State*, 3 Comp. Law Jou. 364 (Del 2005).
[60] *Supra* note 1 at 62.
[61] Michael L. Rustad & Thomas H. Koenig, *Rebooting CyberTort Law,* 80 Wash. L. Rev. 335, 406 (2002).

this safe harbour. Section 67B of Information Technology (Amendment) Act, 2008 states that anyone who publishes or transmits, or causes to be published or transmitted, material in any electronic form which depicts children engaged in sexually explicit act or conduct is punishable on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees, and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.[62] This clearly shows that liability is imposed on the intermediaries in the case of child pornographic content in the site; reading 67B in conjunction with section 79 shows that the former section creates a chink in the safe harbour provision provided in the later. Comparing it with US law and UK law it can be noticed that it is a case of strict liability as the word 'knowingly' frequently used in both of their legislations is avoided in the amended Act to convert it from a with-fault liability to a strict liability clause.

Despite amendments, lacunae continue to remain in the Act. What standard of knowledge has to be adopted hasn't been made clear. Also the issue of due diligence has not been made clear in the event of which the degree of care exercised would still be subject to interpretation by courts. The 2008 Amendment Act has also made the intermediaries strictly liable in situations where the content involves pornographic materials depicting minors or that can induce minors into sexually explicit acts. The Indian law still seems to want to exercise a tighter check on the intermediaries unlike countries like US where judicial interpretation has played a role in expanding the ambit of the immunity granted to intermediaries.

2.4 Comparing the Regimes

The US regime presents an approach which is moving towards a no-intermediary liability system which immunizes the intermediary even when it had knowledge of the obscene content being uploaded. From a with-fault liability system, there has been a transition to a relaxed system in which intermediaries are provided enough safe habours thus expecting them to indulge in self-policing measures. The US regime presents the most lax regimes of the three with the Indian system at the other end of the spectrum. The EU E-Commerce Directive aims at a policy of with-fault liability where the knowledge and intention of the intermediary is taken into consideration while fixing liability as seen from the Swedish Pirate Bay case. The non-binding nature of the EU regime has been a major flaw as it imposes no obligation on the member countries to implement it. Therefore, varying degrees of intermediary liability has been observed in various jurisdictions. This poses problems of jurisdictional issues producing results quite contrary to what the EU Directive wanted to achieve through laying down guidelines for a uniform approach.

The Indian stand on intermediary liability is similar to the EU position. Legislative amendments have resulted in a transition from a strict intermediary liability regime to that of a fault-based liability system in most of the cases. However, the Indian position differs from that of the other two regimes in the case of child pornography. Unlike EU and the US which provide blanket immunity for intermediaries, the Indian law still holds intermediaries strictly liable for any depiction of child pornography irrespective of knowledge or intent on the part of the intermediary. Unlike the other two which gives substantial freedom to the intermediaries to carry out their functions effectively, the Indian regime does not give any leeway for the intermediary when it comes to child pornography.

3.0 Towards Evolving an Ideal Regime

The rationale given for imposing intermediary liability is that the intermediary is in the best position to sanction or avoid misconduct on the internet. This raises the question of whether the intermediary be held responsible just because the primary malfeasors cannot be controlled directly and there exist intermediaries who can directly control it?[63] Is the 'ability to control' the criterion on which liability is to be determined?[64] Holding the intermediary responsible involves normative and fault-based notions of responsibility. The under deterrence of subscribers has led to expanded liability for ISPs. Just because ISPs are able to prevent subscriber misconduct cheaply does not mean that they should be burdened with the cost of preventing spread of child pornography and if unsuccessful, pay damages and have criminal liability imposed on them. The Article states that this completely takes away the focus of preventing harmful or illegal conduct and makes it a situation of who shall bear the costs.

[62] Information Technology Act, Section 67B (2008) (In.).
[63] Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 Wm. & Mary L. Rev. 239, 303 (2005).
[64] Rosa Julia-Barcelo, *Liability of Online Intermediaries: A European Prespective*, E.I.P.R. 1998, 20(12). Rev. 453, 459 (1998).

If the effect of the regulation of the intermediary is likely to result only in a shift from that particular medium to another without preventing the misconduct, then the cost of the regulation would be a loss.[65] Imposing liability on intermediaries makes sense only if such a regulation would prevent the spread of child pornography on the Net.

Further, this sort of strict intermediary liability should be done away with as market incentives already exist for the intermediary to regulate content.[66] Many argue for imposing strict liability on them than providing a 'safe harbour' by providing immunities to their actions. The argument has been framed in such a manner that such a measure would result in curbing the exposure of children and minors to the corrupting influences of paedophiles running free in the internet. A strict liability framework is however not necessary as in a normal market setting, the internet intermediaries would be a self regulating group. This is observed in a varied form in the video sharing site Youtube[67] where the content containing material inappropriate is removed upon discovery even if they have no obligation as such to regulate it. In the internet world the numbers of regular users far outnumber the number of paedophiles. Where a host caters to a wide variety of consumers, the opportunity cost of catering to the interests of a particular section would be higher and wouldn't balance the net benefits derived. Only a section of the population is interested in child pornography; this increases the risk for a computer service that it will lose subscribers such as parents who are concerned about children's access and other people who prefer to visit cleaner sites.[68] Intermediary liability would be an effective tool only in cases where the intermediary profits from the misconduct.

Imposition of strict liability is not feasible as it might sometimes result in weeding out of even content with positive social value. The case of LiveJournal, a popular Web journaling site suspending and deleting a number of its user accounts for sexual content illustrates the point of too much censorship. It had merely blocked all those users whose profile pages had any reference to sex or sexual activity. A Harry Potter fan community which contained fan fiction with adult content-rape and incest were also cleansed. LiveJournal's argument was that they had to exercise an abundance of caution which required its staff to suppress anything which might appear to be offensive in any manner.[69]

If a regime of strict liability is imposed on the intermediaries, it can lead to a situation where in order to prevent further financial obligations and criminal offences, the services provided by the intermediaries would be restricted which in turn would stunt the growth of the still to mature industry. The same policy can also affect the right of freedom of expression as a highly regulatory mechanism would remove content which has the lightest chance of bringing liability on the intermediaries. While at the same time an industry which is regulated by the state will experience severe censorship which would directly affect the freedoms of the citizens in the internet.[70] Also there is no way to develop a fool-proof method of determining legal liability as software can merely filter certain words or block certain content. But the offensiveness always depends on the context. An automated machine cannot determine whether a message would be defamatory, invades privacy of another etc.[71] It is not really possible for them to look into the nuances of law and social values which differ from place to place.[72] Also, if the effect of regulation is merely a shift from one particular intermediary to another which has a relatively lax regulation in place, then the cost of regulation is a loss. For instance, imposing a liability on an ISP would result it in employing very strict filters which would cause the customers to shift from using that website to another one which has a lenient policy of filtration.

A with-fault liability scheme seems a better option than strict-liability. However, knowledge standards provided by a with-fault liability scheme also prove to be deeply problematic as if constructive knowledge is the standard, ISPs would be forced to over-regulate so as to escape liability. An actual knowledge standard seems to be viable as it imposes liability on ISPs if they fail to remove materials which they know to be illegal only. This eliminates the over-deterrence problem but would lead to no regulation at all as ISPs have no incentive to engage in monitoring content.[73]

Some sort of self-regulation regime as proposed in the 1999 Multi-annual Action Plan of the European Union for combating illegal and harmful content on Internet is required as the intermediary who has the ability to develop the technical standards has to be made a party in finding out a balanced approach between free speech and the need for law enforcement.[74]

---

[65] *Supra* note 63 at 266.
[66] *Supra* note 63 at 306.
[67] http://www.youtube.com/
[68] *Supra* note 26 at 174.
[69] Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 Geo. Wash. L. Rev. 986, 998 (2008).
[70] Dr. S.V. Joga Rao, Law of Cyber Crimes and Information Technology Law 243 (2004).
[71] Assaf Hamdani, *Who is Liable for Cyber Wrong*, Cornell Law Review. Rev. 901, 936 (2002).
[72] *Supra* note 64.
[73] *Supra* note 71.
[74] *Supra* note 7.

Internet intermediaries should however also be made responsible to keep track of the users and IP addresses that use the site. This would allow the authorities who are searching the sources of paedophilic content to find and track them. If internet intermediaries are made liable, they would remove the content before it is even published and this would not prevent paedophiles and child pornographers from carrying out their activities as they would shift to another medium. In order to protect children against pornography, authorities have to find and curb the sources of child pornography and proper training and awareness have to be given to the ISP to have proper codes of conduct and also cooperation with the authorities. Application of the least cost principle will not allow the law makers to achieve their objective of protecting the children from child pornographers and paedophiles. And imposing damages on ISP would not prevent child pornographers' activities from reaching the children and them accessing the content. When a medium of pornography in the internet is restricted, like a leak in a dyke, a new hole is bound to open up. Hence proper training and awareness for the ISP is very much necessary while at the same time the ISPs should be held accountable to keep record of the activity in their domain than imposing liability on them for the contents. The state should hence concentrate on formulating laws which would curb the activities of the child pornographers than imposing unnecessary liability on the intermediary service providers.

4. Conclusion

Internet intermediaries are an essential component for the normal functioning of the internet and its various subsidiary services associated with it. However with the widespread coverage and ease of use, internet intermediaries have also became a platform for various anti-social elements to peddle their trade, especially the heinous crime of child pornography. In the early stages the governments and state machineries tended to hold intermediaries liable for having child pornographic content to mitigate and regulate the trade under the assumption that holding intermediaries liable would promote the same to regulate them. This regime however later showed a change in character as the results of the former policy had far reaching consequences. The United States of America adopted a policy of freeing intermediaries from the chains of liabilities itself in case of third party content while the nations of the European Union are showing varying degrees of tolerance towards intermediaries hosting offensive third party content. The European E-Commerce Directive was a welcome gesture as it laid down the guidelines that were expected to be followed by the members. The Directive adopted a regime of fault based liability. The Directive however has not been fully implemented as it is observed that many of the countries yet have to follow the guidelines. The developing countries like India still implement a policy of strict liability on the internet intermediaries, especially in the case of child pornography. This, however, is not ideal for the proper functioning and regulation of the internet as a strict liability regime can curtail or encroach upon various freedoms of the granted to the citizens and at the same time prevent further expansion of the intermediary services in the country. The developing countries also should evolve a policy of fault based liability as it is economically more feasible and would not affect the rights of citizen as well.