Internet Intermediaries Liability and the Perils of the Internet in Tackling Digital Copyright Infringements in India

Paramita Choudhury

Assistant Professor, School of Law, Galgotias University, Greater Noida, Uttar Pradesh, India

paramita.choudhury@galgotiasuniversity.edu.in

Sayan Das

Assistant Professor, School of Law, Galgotias University, Greater Noida, Uttar Pradesh, India

sayan.das@galgotiasuniversity.edu.in

Abstract

In the last decade, the consumption of the World wide web in India has expanded significantly. In terms of the number of users, India is one of the most important marketplaces for many worldwide technology businesses. While the rising usage of the Internet has pushed the expansion of the modern economy, and democratised accessibility to information, it has also given birth to significant policy concerns around the necessity to address harmful online material and behaviour. "Intermediary liability" is the central issue in this dispute. Is it appropriate for service providers to be held liable for the actions of third parties that use their services to transmit, transport, or distribute user content? It is an issue of balancing the rights of Internet users and intermediaries, as well as ensuring the digital environment is secure for everyone and that destructive behaviours may be penalised.

The world has long acknowledged the necessity of a Virtual Copyright Law as technology, and in especially, digitalization, has progressed. Existing Copyright legislation has changed in light of the global trend toward digital data preservation, which necessitates the protection that copyright law already provides. Rethinking copyright law's key notions was necessary to keep the digital record of society moving forward. Technology makes the digital data widely accessible, which can lead to abuse of labour in a free flow of knowledge in society, since once this electronic record is put online, author loses all control. As a result, because the Copyright Act has been updated to reflect the digital era, the law allows its owners some negative rights to prevent others from performing activities related to their work.

In recent legislative discussions, both internationally and in India, the role of Internet intermediaries in facilitating or reducing harmful activity in the online environment has received much attention. Disaggregated suggestions for reforming current law and policy in India have emerged. Three questions are being addressed in this paper: what entities are all being decided to seek to be regulated, what harms are being cited as reasons for regulation, and what commitments are being levied on Internet mediators to ameliorate those harms. This article attempts to answer all three of these questions. Increasing duties on some sorts of intermediaries exist on the horizon, albeit the means and technique by which they are being imposed are frequently in dubious. It's time to revisit the legal framework for intermediary responsibility in order to better regulate the internet ecosystem and better understand the roles and duties of various types of intermediaries.

Keywords: Copyright Law, Internet Service Provider (ISP), IT Act, 2002, Intermediary Liability, Safe Harbour.

Number: 10.14704/nq.2022.20.9.NQ440012 Neuro Quantology 2022; 20(9):100-109

Prologue to the concept of Internet Service Provider (ISP)

For the corporate world, the Internet is a double-edged sword. Firms in the digital content delivery industry are interested in advancing network technology in order to improve the sustainability

and quality of the digital material they distribute. There has been a rise in IPR violations as a result of the expansion of this technology. Copyright infringement are more likely to occur as broadband speeds grow, as this facilitates the dissemination of digital content more quickly. Unauthorized high-speed and simultaneous multi-source data transfers are made possible by the development of technical advances like bit torrent in a broadband context. This type of technology has the potential to be a tool for unlawful copying and dissemination of protected information while also providing new opportunities for businesses. Increases in the scope and frequency of infringements of intellectual property rights (IPR) are a natural consequence of the rapid development of network and Internet technologies. The Internet, despite copyright concerns and other problems, is lauded as one of the greatest technologies ever since industrialization and an essential economic channel for the future. According to both academic and real-world evidence, the Internet is a need in virtually every aspect of modern life, including business. Instead of abandoning the Internet, more and more people are urging for answers to the escalating copyright issues.[1]

ISPs also provide connection software using a central server, such as live sharing applications or internet messaging services, which have more specialised tasks. Pure peer-to-peer networking, or decentralisation, refers to programming that does not need a central server. Copyright holders are particularly concerned about ISPs' more recent features.[2]

The many services provided by access providers are critical to the operation of the Internet. It is common for ISPs to have the authority to block down mails and webpages under the contracts they sign with their clients.[3]

Research Objectives

1. To know the concept of Internet Service Provider (ISP),
2. To analyse the notion of "Safe-harbour", and
3. To evaluate the clarity on section 81 overriding section 79 of IT Act.

Research Question

According the Information Technology Act 2000, may an internet service provider be held accountable for copyright infringement?

Research Methodology

The researcher has relied on secondary sources. A variety of sources, including books, journals and articles, are used to get this information.

The Function of Internet Service Providers in Online Communication

Direct, vicarious, and contributory infringement are all grounds of culpability for copyright violations. Any violation of a copyright owner's exclusive rights might be considered a direct infringement. A person is held liable for an infringement when he or she fails to prevent it when he or she has the potential to do so and is actively benefiting from it. In all of these views, an individual will be held accountable regardless of his or her mental state or purpose. A person is held liable for an act of infringement if they have knowledge of the infringement and take part in it directly. Is there a standard by which service providers may be held accountable for their actions?

Web site construction and hosting are among the services provided by Internet service providers (ISPs). To have an Internet presence, an ISP must have access to the necessary hardware and telecommunications lines. The chain of intermediary service providers involved in

[1] R. Muruga Perumal, Copyright Infringements in Cyberspace: The Need to Nurture International Legal Principles, International Journal of The Computer, the Internet and Management Vol.14 No.3 (September-December, 2006) pp 8-31.

[2] Okitikpi Toritseju, Liability of Internet Service Providers (ISP's) For Copyright Infringement in The Nigerian Context, (Jun. 2, 2022, 09:15 PM), http://www.nigerianlawguru.com/articles/intellectual%20property%20law/LIABILITY%20OF%20INTERNET%20SERVICE%20PROVIDERS%20IN%20NIGERIA.pdf.

[3] Thilini Kahandawaarachchi, Liability of ISP for third party online copyrights infringement: A study of the US and Indian Laws, journal of Intellectual Property Rights, Vol 12, pp 553- 561, Nov 2009.

rendering a work available through the Internet necessitates the usage of a variety of intermediaries. A person who wants to build a web site would initially register for a web host and then add weblogs to his website, which is situated on the web server-an extremely massive flash drive that is reachable through the Internet. Once they have been posted to the server, the files can be accessed by anybody with an Internet connection. The Internet can be accessed through an access provider. To go from host to end user, the documentation passes through the network structure of an internet provider, which in addition to supplying the actual means to convey a signal, also transmits and routes it to the chosen receiver. These services are often provided by a single legal organisation. A third-content party's is sent or disseminated by ISPs, but they do not start or participate in any choice to disseminate a specific piece of content.

It is an ISP's responsibility to provide two primary services: (1) Website creation and hosting, which is performed by a company that offers server space and management to individuals or businesses; and (2) Internet access, which is performed by a company that makes it possible for an individual or organisation to connect to the Internet.[4]

Evaluating the ISPs' legal culpability

ISPs are a tempting target for regulatory action. The rationale for this is both practical and moral. Because they function as a middleman, ISPs have some degree of influence over what third parties do. By using their monitoring and surveillance capabilities, they may also be deployed in accordance with regulations in the phase just before an offence is committed, thereby reducing the quantity of criminal and delinquent behaviour. There are two reasons why it is difficult to suit major wrongdoers. If the principal wrong-doers are too many, living in a country where it's tough to make fair evaluations about gains or deficits while remaining anonymous and execute, or if they have no attachable assets, it is extremely difficult to pursue them for damages. Internet service providers on the other hand tend to be smaller in number yet have more financial resources. Holding Internet service providers (ISPs) responsible for copyright infringement perpetrated by their customers is not without risks. People who argue against putting ISPs on the hook because of the difficulty of patrolling the Internet typically point to the impracticality of doing so.

Now, the issue that has to be evaluated is, ***"How far may such intermediaries be held accountable for any illicit or scrupulous material, product, or service that was put on their site, forum, or board by a 3rd party, and to what degree could they be held liable?"*** Because of the exponential expansion of the Internet and the ease with which anybody may access the private and confidential information of others, there has been a recent uptick in the number of crimes committed online in modern times.

Involvement of intermediates in India

The Internet's right to openness of expression relies heavily on intermediaries, who are commonly seen as important parts of the wheel. In order to keep the wheel turning, most major governments throughout the world have enacted legislation to restrict the liability of intermediaries.

Who are the Intermediaries?

As per the Information Technology Act 2000, intermediaries are defined as those who act as a conduit for information. According to the provision, "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, web-housing service providers, search engines, online payment sites, online auction sites, online marketplaces, and cyber cafes".[5]

Services provided by intermediaries enable the end user to access internet content. Here are the people that are a part of this chain:

[4] Raman Mittal, *Online Copyright Infringement Liability of Internet Service Providers*, Journal of the Indian Law Institute, vol. 46: 2.

[5] Sec 2(1)(w), Information technology Act, 2000.

- An internet service provider (ISP), such as Airtel or MTNL, helps consumers connect to the Internet via wired or wireless means.
- Users may use search engines such as Google and Bing to search for particular information on the Internet and get connections to websites that have relevant material for the search keywords they entered.
- Web hosts, such as Godaddy.com, are companies that provide server computer storage space for the data of various websites so that consumers may access these websites.
- Social networking sites like Facebook and Twitter, blogging platforms like Word press, auction sites like eBay, and payment systems like PayPal are examples of interactive websites. In a typical online transaction, there are a number of middlemen involved.

It was the IT (Amendment) Act of 2008 that added this new definition of "intermediaries," replacing the one from the original act.

According to the definition, an intermediary is anyone who provides services related to electronic messages, such as receiving, storing, or transmitting them electronically.[6]

Information and Technology Act, 2000: Section 79 & its relevance

When it comes to the Internet, so-called "Safe Harbour" protections shield companies and individuals that furnish the fundamental architecture from legal liability for the activities of other parties who utilise that system for their own purposes. These people and businesses are also known as "intermediaries." If their customers use the Internet to commit illegal acts such as drug trafficking or other crimes, Internet service providers (ISPs) are not held liable. Similarly, cloud service providers (CSPs) are not held responsible if their customers hold unauthorised information on their web server. E-commerce channels are not held responsible if their customers sell counterfeit goods.[7]

Intermediaries are immune from responsibility under Section 79 of the 2000 Information Technology Act. Third-party information, data, and communication links provided by intermediaries shall not be held accountable by them. Only those situations where the intermediary works as a conduit and does not take part in the creation or alteration of the facts or content are protected by the *"safe harbour"* provisions of the Act. As a condition of getting safe-harbor protection, the intermediary must remove any illegal content from its computer resources upon notification from the competent sovereign or its body or upon gaining actual information.[8]

By way of the Information Technology (Amendment) Act of 2008, software companies and industry associations requested that user contributed material be shielded from liability. An auction site CEO was detained when a user put an indecent MMS clip up for trade on the site, prompting this investigation. An intermediary is required to follow the Central Government's

[6] Salient features of the Information Technology (Amendment) Act, 2008, (Jun. 5, 2022, 11:30 PM), http://www.indiancybersecurity.com/amendment_itact_2008.php

[7] Ikigai Law, Visual-Guide to Existing Safe Harbour Provisions, (Jun. 7, 2022, 01:30 AM), https://www.ikigailaw.com/current-safe-harbour-provisions/

[8] *See* Section 79 in The Information Technology Act, 2000

There are instances in which an intermediary is exempt from responsibility. A third-party information, data, or communication link made available or hosted by an intermediary is not subject to an intermediary's liability, regardless of what is stated in any currently in effect statute.

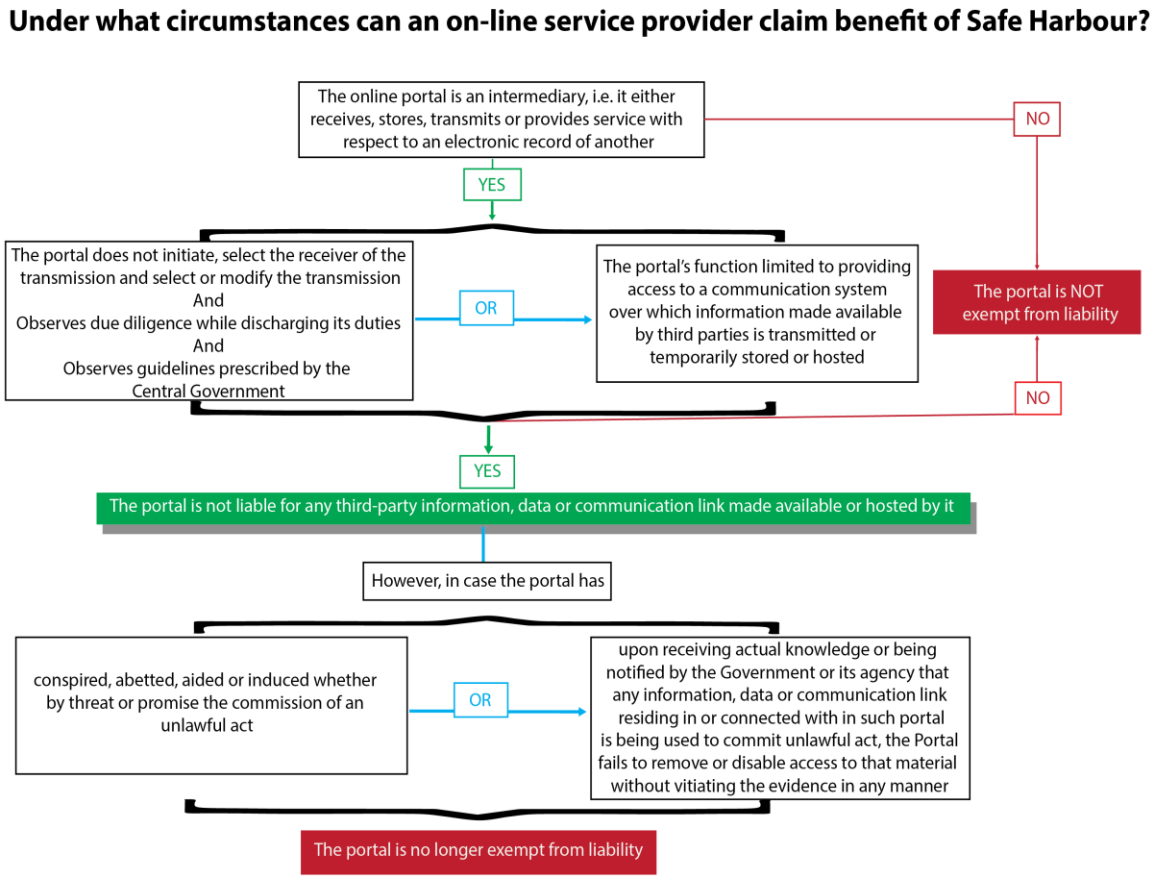
If the intermediary's role is limited to providing access to a communication system through which information provided by third parties is transmitted, temporarily stored, or hosted, or if the intermediary does not initiate the transmission, select the receiver of the transmission, or modify the information contained in it, the provisions of subsection (1) apply; and if the intermediary does not, the provisions of subsection (2) apply;

The provisions of subsection (1) do not apply if the intermediary has conspired, abetted, assisted, or induced the commission of the unlawful act by threats, promise, or authorise; or (b) upon receiving actual knowledge, or on being notified by the appropriate government or its agency that any information, data, or communication link residing in a computer resource, controlled by the intermediary is being used.

Explanation.

"third party information" refers to any information handled by an intermediary in his or her role as an intermediary.

recommendations and use due care when performing its obligations under the Act.[9]



Source: Ikigai Law, *Visual-Guide to Existing Safe Harbour Provisions,* https://www.ikigailaw.com/current-safe-harbour-provisions/

Judicial Activism and Information Technology Act

The Information Technology Act has been a hotly debated piece of law ever since it was introduced in October 2000. Even after 13 or so years, the legislation was able to accomplish its goal elicit, substantial for both the juridical and wider populace have their say about this. Various problems, weaknesses, and traps are believed to be contained inside, including the inability to effectively combat cybercrime and the arbitrary restriction of people civil freedoms.

To make matters worse, in 2008, the now-famous Section 66A was added to the Act. For transmitting "offensive" this section outlines the penalties for using a computer or other electronic messaging tool, such as a cell phone or tablet. For a conviction, the maximum penalty is three years in jail and/or fine. This part has a major problem at the heart of it is the ambiguity around which constitutes "offensive" behaviour. The term has a broad sense and may be interpreted in many different ways. For example, the cops may arrest someone under Section 66A if authorities consider into account the viewpoint of the party who made the complaint, even if it is benign to the complainant.

[9] Avnish Bajaj v. State, 150 (2008) DLT 769.

Both Section 66A and the Information Technology (Intermediaries Guidelines) Rules, 2011, have come under fire. However, while Section 79 exempts intermediaries from responsibility in some situations, the Rules weaken these exemptions and compel intermediaries to review material and implement online censorship measures Web sites can be blocked without sufficient notice or publishing under the Information Technology (Procedure and Safeguards for Blocking Access to Information by Public) Rules, 2009. Natural justice safeguards are violated in the blocking procedure, which is kept secret and unexplained.

Because it violated Article 19(1) (a) of the Indian Constitution and did not fit under the definition of "reasonable limitation" in Article 19(2), Section 66A of the Information Technology Act of 2000 was repealed completely. In *Shreya Singhal v. Union of India*, the Supreme Court ruled that Section 66-A of the Act prescribes penalty for transmitting obscene remarks via communication service.[10] As stated in Section 66A, internet freedom is limited by statute, which is confusing in its language and difficult to understand. Even more problematic, the Intermediaries Guidelines Rules compel private intermediaries to subjectively evaluate undesirable information. Section 79 of the IT Act exempts intermediaries from responsibility, but these new rules weaken those protections and impose unrealistic deadlines for removing harmful information. Articles 14, 19, and 21 of the Constitution are thus deemed to be in violation of Section 66A and the Rules, and the petitioner seeks to have them declared such.[11] As stated in Article 19(2) of the Constitution, "reasonable limits" on fundamental rights may be imposed, however the ambiguity of 66A's terminology encourages obvious violations.[12] Complainants with hurt emotions and police officers have the right to arrest and threaten criminal charges against speakers and authors under 66A because of the ambiguous and imprecise stated violations. Section 66A contains a large number of offences that do not even come within the constitutionally allowed categories of limitation set out in Article 19(2). According to Intermediaries Guidelines Rules, private internet service providers must make legal assessments and effectively restrict content that is not clearly defined. According to the Information Technology (Procedure and Safeguards) Rules, 2009, online pages can be blocked without sufficient publishing or public notification of the reasons for banning. Natural justice provisions guaranteed by the constitution are absent from the blocking procedure, which is conducted in secrecy.[13]

UTV Software communications ltd. vs. 1337x.to, 2019 in cs(comm) 724/2017

An ex-parte judgement by the Delhi High Court has resulted in India's maiden dynamic injunction, allowing the injunctive relief bearer to utilize the court ruling to ban content-infringing webpages without having to file new lawsuits for each incident of violation. Remedy arises in the form of an injunction targeting rogue services that distribute unlicensed copies of cinematographic movies to the general public. However, neither Copyright Act of India, 1957, nor even the safe harbour concept, which applies to intermediaries underneath the statute of Information Technology, 2000, could the accused websites claim any immunity from displaying copyright violating content, according to the Court.[14] Furthermore, the Court ordered the Ministry of Electronics and Information Technology and the Department of Telecommunications to look into the potential of creating an effective and technically viable strategy for cautioning content infringing audiences of their rights to challenge their actions.

Fact of the case

This case was one of a slew of lawsuits brought by firms that create material, produce films, and distribute them all over the world, as well as in India ("Plaintiffs"). Plaintiffs requested an intervention to prevent the Defenders from

[10] Shreya Singhal v. Union of India, (2013) 12 SCC 73.
[11] Rajeev Chandrashekhar v. Union of India, W.P.(C) No. 23 of 2013.
[12] Common Cause v. Union of India, W.P. (C) No. 21 of 2013.
[13] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
[14] Section 79 of the Information Technology Act, 2000 provides for intermediary liability and safe harbour exemptions to intermediaries.

disseminating to the public unauthorized authority the Plaintiff's copyrighted creations in film making. As non-contesting parties against whom no redress was requested, a number of internet service providers ("ISPs") were named as defendants in the lawsuits, including John Doe defendants ("Defendant Websites"), MeITY, DoT, and many recognised websites ("Defendant Websites").

For the Plaintiffs, enabling the unlawful viewing and illegal material downloading, as well as advertising on the Defendant Websites' websites, was a necessary part of their business strategies. In order to view or download copyrighted information, the end user was sent to a host area by these websites, which operated under the guise of privacy. When one URL of the Defendant Websites was banned, the main argument made by the Court was that the Accused Webpages replicated and proliferated. Defendants were found to have a serious aim of infringing or facilitating the infringement of copyrights by the Plaintiff. To get an injunction banning the main website, the plaintiff drew on precedents set by courts in numerous jurisdictions. The Plaintiff seeks an appropriate relief in the form of an injunction through this suit in light of international precedent and the growing necessity in a technologically driven society.

First and foremost, the Court-appointed Amicus Curiae said, was the question of whether Defendant Web pages could be considered 'flagrantly infringing online places.' Site-wide bans may only be enforced when there is sufficient evidence to show that a website is disseminating copyrighted or pirated content, and such evidence must be presented by the Plaintiff. It is especially important to exercise caution when a website hosts both illegal and legal third-party information. There were three steps of verification in Eros International Media v. BSNL Suit No. 751 of 2016, developed by the Bombay High Court, to back up the Amicus' claims, and these steps are listed further in this evaluation. Proportionality rules must be followed by courts when issuing blocking orders, so that internet access is not harmed. Finally, the Amicus argued that the injunctions would be worthless if the infringers were operating from many domain names, as the Amicus argued. Under Section 151 of the Code of Civil Procedure, the Court has inherent authority to impose dynamic injunctive relief concerning rerouted or mirrored websites.

According to the Delhi High Court, the *"dynamic injunction"* derived from particular Singaporean law requirements. Court concluded that it could construct a comparable remedy under Section 151 of the CPC and that the plaintiffs may use the Order 1 Rule 10 of the CPC to seek an injunction against additional websites.

The court, on the other hand, believes that the judicial system should not be required to continually monitor and adjudicate on the legitimacy of such affidavits. As a result, the order gives the joint-registrar of the Delhi High Court, who serves in an administrative position, the authority to decide whether additional websites should be added to an existing banning order There are a number of special rules that govern this case: Section 7 of the Delhi High Court Act, 1966; Chapter II, Rule 3(61) and Rule 6 of the Delhi High Court Rules 2018. A disgruntled party can also challenge the joint registrars' orders under the same rules.

Last but not least, the court 'instructs' the Ministry of Electronics and Information Technology and the Department of Telecommunications, both of which are as well accusers in this particular instance, to perceive a proposal that they can step up with a strategy for a graduated rebuttal arrangement. Under this plan, persons who connect "pirated content" can be informed of the following by their Internet service providers, and if they do not abstain from persisting such doings, they may be subject to fine. The Court was of the opinion that this would go a long way toward promoting legitimate material and speeding the pace of 'Digital India', as well as going a long way toward reducing the amount of stolen content and activity on the dark web.

Copyright Act and IT Act: Integrated or Separate

Until recently, the Copyright Act of 1957 did not include a provision for the responsibility of Internet service providers (ISPs). 4 Until Section 79 of the Information Technology Act of 2000

was enacted, ISPs were unable to be held liable for their customers' actions. Section 79, on the other hand, exclusively shielded service providers from responsibility deriving from the IT Act 2000 and its legislation and standards.[15]

Section 79 of the IT Act of 2000 and its rules and regulations provide protection to service providers exclusively in cases of responsibility under those laws.[16] This meant that the service providers could not claim immunity from other types of legal liability. For example: the Copyright Act of 1957 is not excluded from the protection provided by Section 79(1) as amended, which means that service providers are protected from liability arising from all statutes (for example, liability arising from Section 79(1) discussed hereinafter). Thus, the threshold of immunity accessible to service providers is significantly increased. The caveat to Section 81 of the IT Act, 2000, however, must be examined when contemplating intermediary responsibility in the context of copyright law.

Additionally, this perspective is bolstered by the High court of Delhi's decision in *Super Cassette Industries v. My space & Another*,[17] when reading Section 81 and the exception, the Court concluded that IT Act provisions may override equivalent laws now in existence, but they may also undermine the interests of copyright and patent owners. Since all other online wrongs that involve intermediaries, such as auctioning, networking services, news distribution, and the posting of pornographic content are explicitly excluded by proviso to Section 81, the Court noted that Section 79 is intended for them. To make both Acts workable, this is the only conceivable harmonic structure of the twin Acts [Copyright Act & IT Act].[18]

Copyright 2012 Amendment Act vis-à-vis the ISP Liability

Those portions of the Copyright Act that pertain to ISPs' legal responsibilities are found in Sections 52(ii)(b) and (c).[19] If a composition or performance is only temporarily or incidentally stored in the technological the procedure through which it is made available to the general population, it is not a violation of copyright. In addition, this is stated in Section 52(c) of the Copyright Code, if a work or performance is temporarily or incidentally stored in order to accomplish it making it easier for people to communicate with each other electronically, it will not include any illegal activity of any kind, if the individual accountable is cognizant or has substantial basis to suspect that the preservation is of an illegal copy. However, there is a case to be made that these limitations are flawed in various ways.

It is argued that requiring an Internet service provider (ISP) to monitor its clients would infringe on their right to privacy. Article 21 of the Constitution protects citizens, basic right to privacy.

Furthermore, it is argued that the use of the ambiguous phrase "reasonable grounds for believing" was done on purpose. To allow judges to exercise their discretion in deciding specific cases, legislators left the door open. As a result,

[15] See Farooq Ahmed, *Liability limits of Service Providers for Copyright Infringement*, Journal of Intellectual Property Rights, 181-190(2003).
[16] Section 79 of the IT Act, 2000.
[17] 2011(47) PTC 49 (Del).
[18] Ibid.
[19] *See* Section 52: Certain acts not to be infringement of copyright. - The following acts shall not constitute an infringement of copyright, namely: (b) the transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public; (c)transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder, unless the person responsible is aware or has reasonable grounds for believing that such storage is of an infringing copy:
Provided that if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work, complaining that such transient or incidental storage is an infringement, such person responsible for the storage shall refrain from facilitating such access for a period of twenty-one days or till be receives an order from the competent Court refraining from facilitating access and in case no such order is received before the expiry of such period of twenty-one days, he may continue to provide the facility of such access.

accuracy has been surrendered for the sake of convenience.

Therefore, we can see that the Indian Copyright Act does not explicitly include service providers' responsibility for copyright infringement. ISPs are free from responsibility under the Information Technology Act of 2000 if they can demonstrate that they were unaware of the alleged act and that they had taken appropriate measures to prevent it. This section does not specify any limitations on service providers' responsibility. Will a service provider be held accountable if he fails to remove illegal content from his network within a reasonable amount of time after receiving a claim from someone asserting copyright on the content accessible on the network? The service provider's claim that he did not know about the copyright infringement in the foregoing circumstances is no longer admissible. Are service providers responsible to the individual whose materials were deleted if they do so on the basis of a false representation made by the person whose content was taken from the network. Service providers in India need to be more clear about their culpability in copyright infringement cases. Sections of the Information Technology Act that cover the financial side of the transaction and the connection amongst an ISP and a 3rd party are essential for identifying the offender. It's possible to bring into Indian law the American notion of contributory infringement and hold anyone who has knowledge of infringing behaviour responsible for the infringing action of another. Indian law protects service providers that take reasonable steps to avoid committing infringements of third-party intellectual property rights. You may end up losing your privacy and having an adverse influence on your life if due diligence requires you to keep an eye on everything you do on the Internet, which may be dangerous. ISPs' primary duty is to construct the Internet rather than serve as a police force, hence there has to be an agreement on the definition of the phrase due diligence. It has been established by US Courts that an ISP must not be ruled accountable for every Internet activity if it acts reasonably.

Moreover, there has been a lot of discussion about the developing nature of internet intermediary liability in 2018 because of the planned amendments to the Information Technology (Intermediaries Guidelines) Act, 2018. Automated filters are mandated under rule 3(9) of the draught regulations for intermediaries in order to help them identify illegal content on platforms.[20] Due to the fact that mediators and their algorithms would subsequently be able to select what information is published online, the draught was met with several complaints. Online copyright might be jeopardised by a regulation that contradicts constitutional law (see the Shreya Singhal Judgment[21]). While this is the most obvious effect, it has various other consequences for the free exchange of creative works online.

The Problems Associated with Preventative Surveillance

As a whole, dynamic surveillance threatens both intermediary immunity and the notice-and-takedown system. According to the safe harbour paradigm, there is no way for a third party to exert control over the material that is being moved across platforms as the intermediaries are only acting as "intermediaries." To qualify for the safe harbour, a third-party intermediary must simply be a conduit for content. Intermediates would no longer be regarded passive intermediaries, but rather companies with complete power over the information on their platforms if requested to monitor it. This contradicts the basis of the safe harbour offered by the government. As a result, it can only be argued that the safe harbour paradigm offered to intermediaries in many countries, such as India, EU, and USA, would not be able to coexist with a proactive monitoring system aided by AI technologies.

[20] *See* (Draft) Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, Rule 3(9) "The Intermediary shall deploy technology based automated tools or appropriate mechanisms appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content." (Jun. 21, 2022, 04:15 AM), https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

[21] *Supra* note 10.

State-mandated proactive monitoring, like its incompatibility with the safe harbour concept, would lead to an unprecedented and hazardous deviation from the Notice and Takedown method, which was adopted by the majority of nations. Rather of allowing users and courts to determine whether or not a piece of material should remain online, intermediaries would utilise auto-filters to determine whether or not a piece of content should remain online, as opposed to the notice and takedown process. The Copyright Act of 1957 grants copyright owners the authority to prohibit automated filtering of copyrighted information online.

Way Forward

There is a need to establish a balance amongst over and under-enforcement when it comes to internet intermediaries and copyright law. Over-monitoring of intermediaries, on the other hand, might lead to the suffocation of innovative and valuable services, limiting market involvement and impeding fundamental constitutional freedoms. The platforms, on the other hand, can become regular supporters of IP infringements (inhibiting digital creation) and the growth of illegal content online if they are not supervised.[22] In order to deal with the problem of an overabundance of notifications to take down information, automated algorithms have been implemented to filter content that might make intermediaries accountable, which has led to their involvement in enforcement mechanisms. Auto-filtering by internet intermediaries has prompted fresh disputes, however the arguments in favour of such automated algorithms are yet to acquire traction. Several reasonable objections against this practise have been stated in this article, some of which have been discussed. Proactive intermediary screening would do more harm than good when it comes to copyright infringements. There is no way this would help increase the amount of original content available online by reducing the amount of copyright violation.

****

[22] Jaani Riordan, A Theoretical Taxonomy of Intermediary Liability in Giancarlo Frosio, Oxford Handbook of Online Intermediary Liability (First ed.) (Oxford University Press, 2020)