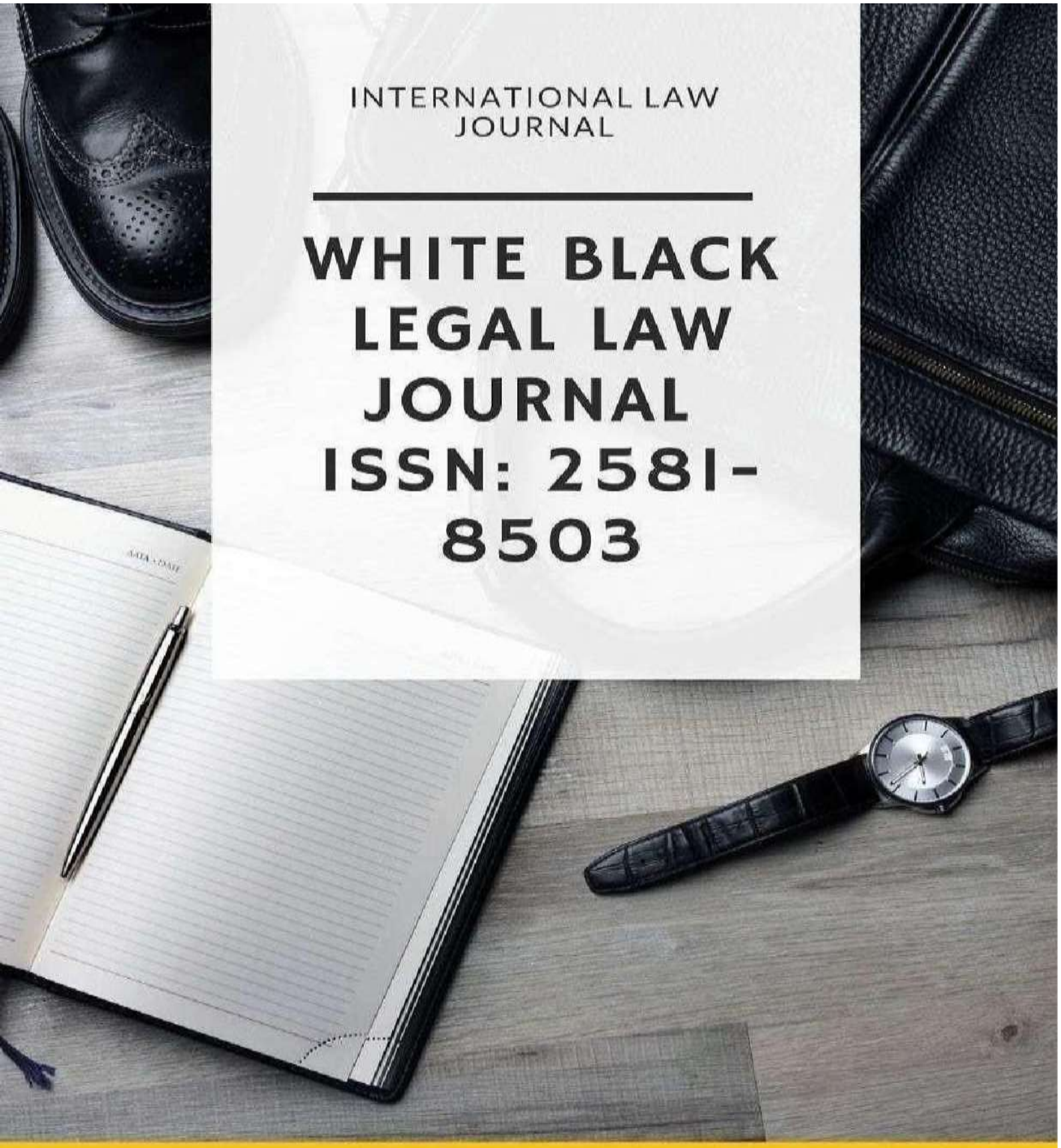

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

COPYRIGHT INFRINGEMENT ON THE INTERNET: A FOCUS ON THE ROLE OF INTERNET SERVICE PROVIDERS

AUTHORED BY - AKSHITA KAUSHIK

Introduction

With transactions occurring over an open network environment, questions are raised as to the liabilities of the carriers of these transactions, should disputes or problems arise.

In the physical world, intermediaries such as publishers are accountable for the content published by the authors. However, in the electronic world, there are some classes of intermediaries (for example ISPs) who carry the data, and do not exercise direct control over the content similar to that of telephonic operators, though, they, potentially, have some, level of control. In the spirit of promoting electronic transactions, it is important to clarify and, where appropriate, limit the liabilities of such intermediaries. It is proposed that intermediaries who are network service providers are not responsible for third-party content to which they merely provide access. On the other hand, it is necessary to ensure that providers do not shirk their responsibilities under the licensing scheme to regulate undesirable content. The legal provision should, therefore, make it clear that it will not absolve ISPs from their licensing obligations.

Section 79 of the Information Technology Amendment Act, 2008 provides for Network service providers not to be liable in certain cases. It reads as-

“For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—

For the purposes of this section, —

a) "network service provider" means an intermediary;
b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;”

However, it is yet worthy to understand how the situation was before the so called "safe harbor" was not present under the Indian legislation.[1] Google is a veteran of several copyright infringement battles in the Western countries. It is most of the times that Google either wins the battles or settles them before judgement. The conventional IP strategy involves negotiating with the copyright owners for the licensing rights before capable of using the rights in their copyrighted work. However, Google approaches different strategy which involves first violating the copyright of a certain content and then later when caught by the copyright holder, negotiate with them for sharing advertising revenues with them. In fact, giving more shock to the copyright owners, Google offers its policy whereby it deems use of all contents as fairuntil the copyright owner informs Google that he no longer wishes to be part of Google's program. This means that the copyright owner can demand for license in turn to use of their content by the Google. This essentially amounts to implied license. Here, it is noteworthy to put a referenc e to the case of *Google v. Field*[2] wherein it was held that the Google would not be held for violating copyright when performing the function of basic search engine. This is because there exists a prevalent practice of industry on the internet whereby the copyright owner could specifically obstruct Google from indexing their website. Thus, it can be understood from this that the implied license defense of Google cannot be applied to those copyright infringements where copyright owners are not in a position to prevent the potential infringers.

When Google was sued by Viacom[3] it applied its usual strategy of playing a defense and safe harbor under the provision of the Digital Millennium Copyright Act.[4] As per the said provision all internet content providers which include search engines are exempted from secondary liability for potential offences if they have complied with the conditions of the safe harbor provisions, viz.:

1. The content has been stored and uploaded by the user;
2. Google must have a policy to bar repeat infringements
3. Google must designate an agent in the Copyright Office to issue "takedown" notices regarding copyright materials.[5]

[1] Jonathan Band & Matthew Schruers, Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act, 20 Cardozo Arts & Ent. L.J. [v] (2002).
[2] Google v. Field, 412 F.Supp. 2d 1106
[3]Viacom International, Inc. v. YouTube, Inc., No. 07 Civ. 2103 at http://en.wikipedia.org/wiki/Viacom_International_Inc._v._YouTube,_Inc. Last seen on April 21, 2025
[4] 118 U.S.C § 512 (c)
[5] Kevin C. Hormann, Comment, The Death of the DMCA? How Viacom v. YouTube may define the Future of Digital Content, 46 Hous. L. Rev. 1345 (2009-2010).

Some Asian countries including Singapore have enacted laws dealing with the challenges posed by the advancement of technology. The Singapore Parliament incorporated various necessary suggestions in their Bill in August 1999 and enacted the Copyright (Amendment) Act, 1999 incorporating into their Copyright Act.[6] This act deals that the third party or the Internet Service Provider cannot be held liable for making copies of the copyright materials on network which are

1. made from another electronic copy from the network,
2. through an automatic process,
3. in response to an action by a user of the network
4. to facilitate efficient access to the materials on the network;

However, this is subject to some conditions which ought to have been followed by the third party of the Internet Service Provider facilitating making of copies of work from internet. The conditions are enlisted as:

1. the third party/ ISP must not make substantive changes/ modifications to the contents while transmitting them as cached copies to the internet users,
2. the third party/ISP must take expeditiously remove or disable the access to the cached copy of the material on internet, in cases where they have received notice from the copyright owner or from owner's authority [Section 193C of the Singapore Copyright Act, 1987]

The provisions in the Digital Millennium Copyright Act of the United States are also similar to the provisions in India and Singapore where the third party/ ISP, facilitating access and making of copies of the copyrighted work, has to be informed about the violation before the liability attaches.

T-Series (Super Cassettes Industrial Limited) v. YouTube[7] (Google)

T-Series sued YouTube alleging that YouTube and Google has made available the copyrighted contents owned by T-Series in the form of music, songs, video clips, etc. without any license or permission from or any payment of any royalty to T-Series. This case was filed in 2007, when the Information Technology (Amendment) Act, 2008 was not in force, which specifically brought the provision of protection of intermediaries from the liability of infringement. An

[6] Singapore Copyright (Amendment) Act 1999amending Copyright Act 1987 (Cap. 63, Rev. Ed. 1999), available at http://www.egazette.com.sg; see also site for Intellectual Property Office of Singapore at http://www.ipos.gov.sg/resource/lu1999.html ; both last seen on April 21, 2025
[7] 2011 SCC OnLine Del 4712

interim injunction was issued by the Delhi High Court against the YouTube restraining them from infringing the copyright of T-Series. According to the Delhi High Court's website, the case was disposed of on 31st January, 2011. The matter was settled between the parties out of court.[8]

Hence, through this case, the Delhi High Court could not decide on whether the online platform (an intermediaries) be held accountable for the contents being published by their users. This status was unclear until the Information Technology Amendment Act, 2008 came into existence.

Enforcement

There would plainly be little point in adopting a national approach to unlawful acts on the Internet. In addition to taking an international approach, we also need to establish the question of who is in fact responsible and liable for unlawful acts on the Internet. Should it be the sender of the information, the service provider, the user or all of them together? The access providers in general claim that they are nothing more than the messengers. Their role should not be compared to that of a publisher, but resembles the role played by telephone companies, which connect callers or interconnect fax and data transmissions. In the Church of Scientology case in Netherlands the court decided that information providers do nothing more than offer an opportunity to publish and that, in principle, they are unable to exercise any influence on, or even be aware of, what people say or are able to say on the Internet. It follows that there is, in principle, no reason to hold service providers liable for unlawful acts committed by Internet users. However, liability could be assumed in a situation in which it is unmistakably clear that a publication of a user is unlawful and in which it may be assumed, in all reasonableness, that this is also known to the service includes the automatic and temporary storage of the third-party material for the purpose of providing access; 'third-party', in relation to a network service provider, means a person over whom the provider has no effective control.

Since it is not possible for the service provider to screen all material before it is made available on the site, it would not seem acceptable for the service provider to be solely liable. Even if he were constantly to monitor all the sites on his server, the provider would never be able to

[8] http://www.medianama.com/2011/02/223-youtube-music-label-t-series-reach-out-of-court-settlement/ ; last seen on April 21, 2025

prevent an infringement and could consequently never avoid liability. Further, more, such a liability would lead to an undesirable form of censorship by the service provider. On the other hand, the service provider is the only person, apart from the information provider himself, who can stop the infringement by closing the site. It would seem to place an unacceptably heavy burden on the holder of the right to have to prove an infringement in court before a service provider is obliged to reveal the identity of the anonymous information provider and close the site. In order to avoid both censorship by service providers and saddling them with an unduly onerous liability, everything possible should be done to trace the source of the information. The source and not the service provider should be primarily liable for the content. However, it is considered reasonable to hold the service provider liable in certain cases and to oblige him in those cases to close the homepage and, on request, lo disclose the identity of the anonymous homepage. It is questionable whether the courts will continue to take the line that the service provider is not liable. The appeal in the Church of Scientology case is pending in Netherlands. The Dutch government has announced that it will take a stance on the legal position of the Internet service providers and present this to the Parliament.

Quite apart from the legal instruments, there are also, of course, technical means of barring undesirable information from the Internet, namely electronic blockades. Users of electronic communication media can block the use .of certain services or the consultation of certain material by electronic means. In the United States, commercial online services such as America Online and CompuServe provide parents with the technological means to deny their children access to certain information. Imposition of Intermediary Liability new information technologies have stimulated a rethinking of the legal rules according to which information intermediaries are held legally responsible for harmful information created by someone else. Penalties might be imposed for defamation or copyright infringement, or distribution of contraband such as child pornography. Intermediaries also might, although the cases have not arisen yet in the United States, face liability for false advertising or fraudulent misrepresentation by facilitating the distribution of false or fraudulent material originated by someone else. Similarly, they might face liability for invasion of privacy if they facilitate intrusion into someone else's private information space or facilitate publication of private information about someone else. And, under present and proposed criminal statutes, they might be liable for distributing child pornography or other indecent material.

Two Competing Views Of Liability Of Intermediaries

Historically, Anglo-American law accommodated two opposing ideas. On the one hand, English law created the tort of libel and distinguished it from the tort of slander in order to impose greater liability on intermediaries who published information likely to harm someone's reputation. The then new print technologies justified a new tort beca.se they tended to expand the scope of injury resulting from stating false information about someone else. Under this developmental strand, intermediaries were subject to greater liability than creators of defamatory communication because the intermediary conduct increased the likelihood of injury and the seriousness of injury once it occurs, According to this strand of intermediary liability, the recently released White Paper from the Clinton Administration rejected recommendations for special provisions shielding intermediaries from no fault liability for copyright infringement, on the grounds that 'they are still in a better position to prevent or stop infringement than tine copyright owner. Between these two relatively innocent parties, the best policy is to hold the service provider liable'.

In *Playboy Enterprises v. Frena*[9], the district court found that the operator of the electronic bulletin board on which third-punk is placed digitized images of Playboy center folds infringed the distribution rights of the content originator, Playboy case . It does not matter that defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement. In other words, intermediaries are subject to no-fault liability. The opposing strand in American law is expressed by the United States Supreme Court's decision in New York Times v Sullivan in which the First Amendment to the United States Constitution necessitated reversal of a judgment imposing liability on the New York Times for publishing an advertisement alleged to defame certain officials in the state of Alabama. The Supreme Court reasoned that the public interest in free expression, underlying the immunity against state regulation of speech, in the First Amendment necessitates curtailing the potential liability of information intermediaries lest they be afraid to provide outlets for potentially controversial views. In that and subsequent cases applying this basic principle, the Supreme Court refined the formula for accommodating the common law of libel with First Amendment immunities. While a number of issues are not clearly resolved after three decades of litigation reaching the Supreme Court, two things are reasonably clear.

[9] Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993)

First, the extreme differences between libel and slander, including no fault liability, presumed damages, and requiring publisher to prove truth rather than plaintiff to prove falsity, are unconstitutional. Second, originators of harmful communications have greater responsibility than intermediaries. These two certainties about the law underpin the first major decision about intermediary liability in cyberspace. In Cubby v CompuServe, holding that CompuServe was not liable for an allegedly defamatory message posted on one of its conferences, the federal trial court reasoned, quoting from a 1959 case absolving a bookstore from strict liability for selling an obscene book, that: "The constitutional guarantees of the freedom of speech and of the press stand in the way of imposing strict liability on distributors for the contents of the reading materials they carry... If the contents of bookshops and periodical stands were restricted to material of which their proprietors had made an inspection, they might be depleted indeed. More recently, the Supreme Court of the United States held that free expression concerns negate statutory liability against a distributor of child pornography unless the distributor is proven to have knowledge of both the sexually explicit material and the age of the performer. Tort law long has recognised that intermediaries obligated to handle all traffic should be immune from liability based on the character of the traffic. Communications law, written into the Copyright Act, offers a useful model for extending such immunity into statute law. The Copyright Act deals with the special position of intermediaries in its specialised privileges for broadcast intermediaries.

For example,
s lll(a)(3),18 provides that it is not an infringement of copyright if a secondary transmission embodying a performance or display of a work is made by, any carrier who has no direct or indirect control over the content or selection of the primary transmission or over the particular recipients of the secondary transmission, and whose activities with respect to the secondary transmission consists solely of providing wires, cables, or other communications channels for the use of others. The legislative history notes that cl (3) intends to grant a privilege to passive carriers.

A similar privilege is given for secondary transmissions to parts of a hotel, apartment house, or similar establishment, but only so long as no alterations is made. Intermediaries in the Gil play a somewhat different role from transmission facilities in broadcast media. Intermediary protection must recognize the necessity of a system operator's selection of classes of communications to conform to its entrepreneurial definition of its product or service niche. It

also must recognise the appropriateness of certain transformations and alterations that occur as part of normal digital processing. One could adapt the language of s 111 to the position of other kinds of intermediaries in the Gil in the following way: the forwarding or transferring of a work infringing the copyright of another is not itself an infringement of copyright if the forwarding or transferring is made or facilitated by an electronic service provider who has no direct or indirect control over the content of the infringing work and whose activities with respect to the forwarding consist solely of providing communications channels, pointers, and intermediate copying at the request of another or for the use of others: provided that the exemption provided by this section shall not extend to sponsoring, soliciting, promoting or adopting infringement as the provider's own. If the common-carrier model were adopted completely, the test for intermediary immunity would he whether the intermediary could be compelled to accept content. In the Web pointer context, the test would be whether the server could be compelled to point to a particular website.

Constraining immunity in that fashion would either extinguish it as a practical matter, or involve the creation of a significant new source of access rights, probably unjustified by the inherently competitive structure of architectures like the Web. Instead, language like that suggested in this section should focus on a lack of control—a standard that fits comfortably with traditional tests for contributory infringement of copyright. Of course, intermediaries also would like to have both immunity and complete freedom to censor and choose their content—in the absence of trade-off not usually found in the law, and not generally desirable as a matter of public policy.

Extend the Cubby Standard

The fault-based "know-or-have-reason-to-know" standard articulated in Cubby, Inc. v. CompuServe Inc.[10], remains one of the most cited formulations regarding intermediary liability, particularly for traditional print-based intermediaries such as bookstores and newsstands. Under this standard, an intermediary is not liable for defamatory or harmful content unless it knew or had reason to know of its unlawful nature. This framework, in many respects, appears adaptable to new-technology intermediaries operating in the digital space. However, significant concerns remain regarding the scope, applicability, and practical implications of this standard in the context of modern internet services.

[10] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991)

Firstly, the Cubby standard is not extended to violations involving intellectual property rights, such as copyright or trademark infringement. In such cases, intermediaries may incur strict liability regardless of their knowledge or intent. If an intermediary reproduces, distributes, performs, or displays infringing material, it is liable even if it neither knew nor had reason to know of the infringement.[11] This sharply contrasts with the fault-based regime applied to defamation or reputational harm.

Secondly, there is doctrinal uncertainty in applying the Cubby framework to modern internet-based intermediaries, especially those engaged with World Wide Web functionalities, such as content hosting, caching, and indexing. The rapid evolution of digital platforms complicates the application of traditional liability norms that were originally devised for passive distributors.

Thirdly, the intermediary's policy choices about content moderation—either actively screening material or adopting a hands-off approach—pose dilemmas for liability standards. The ruling in Stratton Oakmont, Inc. v. Prodigy Services Co.[12], exemplifies the punitive outcome of classifying intermediaries as publishers merely for exercising editorial control to eliminate harmful content. This discourages socially beneficial moderation by increasing legal exposure for platforms that attempt to self-regulate. This concern mirrors the broader criticism of granting immunity solely to those intermediaries who take no affirmative steps to monitor or control content. Such a regime arguably incentivizes willful blindness, protecting only those who adhere to a "hear no evil, see no evil, speak no evil" model.[13]

In light of these challenges, reconsidering the Cubby standard and adapting it to nuanced technological realities is essential. A balanced approach should recognize degrees of involvement, technological capabilities, and good-faith moderation efforts by intermediaries, especially in contexts involving intellectual property and harmful content.

Minimise Prior Restraint

The problem with the present law is that de facto prior restraint occurs because of the combination of the rules of intermediary liability for copyright infringement and the economics

[11] (Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552, M.D. Fla. 1993).
[12] Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. 1995),
[13] Balkin, Jack M., Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 NYU L. Rev. 1, 2004.

of intermediaries in the information infrastructure. The intermediary imposes prior restraint at the first hint of a controversy over mutual property. The point is not only that the intermediary may be subjected to an injunction or criminal prosecution in advance of the dissemination; the point is the possibility of a damages judgment effectively works to shut down the dissemination just as effectively as an injunction or incarceration of the intermediary would. What is needed is to give the intermediary more guidance as to what exposes it to liability and what does not. The law could insulate an intermediary from damages exposure unless and until it is presented a neutral determination that a particular item is infringing.

One obvious way to do this is to protect intermediaries from liability unless a judgment has been entered. In particular material infringes and that it is feasible for the intermediary to screen out the material, but the approach would not adequately protect the interests of copyright holders. It takes a long time to get a judgment on the merits in most jurisdictions and continued availability of infringing materials while the litigation process proceeds could result in substantial irreparable harm to copyright holders. The need to prevent irreparable harm pending litigation is not a new challenge to legal systems.

Federal Rule of Civil Procedure 65(a) is a prominent example of a procedure that allows a threshold judicial determination as to whether an activity should be stopped or allowed to continue pending unless there is a complete adjudication of competing claims. It allows a 'temporary restraining order' lo be issued summarily, and ex parte in some circumstances, when the requester can show that irreparable harm will be established by waiting for a full hearing. The law relying on the protections available under injunction procedures like r 65, could shield intermediaries from liability unless and until some kind of court order has been issued, relying on judicial procedural rules to protect against judicial or partisan overreaching in obtaining such an order.

But there is another problem to be addressed before temporary restraining orders are viewed as the solution to the de facto prior restraint problem. An injunction, whether final, preliminary, or temporary is an archetypal prior restraint, if the orders distribution of controversial material to stop. This problem could be avoided by recognising the flexibility of injunctive remedies.

There is no reason that a preliminary injunction representing the needed judicial determination of probable cause or probability of success on an infringement claim must prohibit

dissemination. Such an order can impose conditional damages for continuing to engage in conduct. In effect, the court presented with a TRO or preliminary injunction application by a copyright holder or victim of defamation or would say, and find probable cause to believethat the accused item is infringing or defamatory and declare that any damages proven on the trial of the merits will accrue from the date on which this order is entered.

Encouraging Closed Networks

A final alternative, implicit in the White Paper's lack of sympathy for the position of intermediaries, is to encourage reliance on closed systems, like pre-Internet CompuServe and NEXIS, rather than newer open architectures like the Internet. A distributor who controls its content faces less risk than a distributor who facilitates access to content controlled by another. Such an approach vitiates the benefits available from open architectures.

On the other hand, as the Gil matures, the advantages of closed networks for protecting intellectual property and discouraging tortious and criminal content may lead to a merger of open and closed architectures. While some role may remain for the original closed networks like pre-1993 CompuServe, America Online, WESTLAW, and LEXIS it is more likely that new Internet technologies will permit certain features of those approaches to exist along the side with traditional open architectures in the Internet. For example, new tools for screening and blocking Internet packets, being feverishly developed to block pornography to stave off federal legislation like the Exon Amendment, can be used to exclude persons who violate community rules. This would enable an Internet-based intermediary to unplug someone as CompuServe or AOL may do now by cancelling an account and password. Supplementing that means of expulsion or denial of entry will be secure payment systems that deny access to certain Internet resources until appropriate payment arrangements have been made. That is already possible now with a combination of Netscape CGBIN scripts and public key encryption. One can be denied access to a particular set of webpages or news groups unless one has an account name and password associated with that particular set of resources. Public key encryption permits either the private transmission of credit card numbers or authentication of an account holder's identity, as is being demonstrated by DigiCash and CyberCash.

Licensing Options For Internet Service Providers

Some countries require ISPs to obtain government-issued licenses before commencing

operations. Other countries impose less burdensome regulatory requirements, permitting ISP operations pursuant to general authorisations. A third category of countries impose neither licensing nor general authorisation requirements on ISPs. What are the differences among these approaches? What are the benefits and disadvantages of adopting licensing or authorization requirement on ISPs, what are the 'best practices' for how the licensing or authorization rules and procedures should be structured?

The Pros and Cons of Adopting a Licensing Requirement for ISPs

The decision to adopt an individual licensing mechanism for ISPs effectively establishes a nation's regulatory authority as the country's 'gatekeeper' to the Internet market. If the regulator adopts requirements for ISPs that are unduly burdensome, restrictive or opaque, these procedures may slow or prevent the entrance of ISPs into a nation's market. The licensing process thus can become a means for regulators to restrict, internationally or not, the market access of ISPs, which will keep costs high and limit the overall growth of the country's communications and information services. To avoid such results, the US and the European Community advocate that countries not adopt licensing requirements in mature and competitive markets. Although this deregulatory approach has many advantages, it may not be appropriate in every market. To the contrary, there may be legitimate reasons for countries to require individual licenses where the telecommunications market is not fully competitive or where the business regulatory and consumer protection framework has not yet been established.

In some markets, therefore, it may be beneficial to provide ISPs with some type of licensing mechanism. In some countries, regulators detail, in the license itself, the rights as well as the obligations of communications service providers. In some instances the license constitutes an actual contract between the regulator and the operator. Consumer protection conditions those related, eg, to price regulation, billing practices, consumer complaint mechanisms, dispute resolution, limitation on liability for service defaults, and mandatory service due to consumers, such as directory services, operator assistance and emergency services) and conditions related to interconnection are frequently described in telecommunications licenses that are issued to carriers in such countries. In Mexico, for example, quality of service standards and targets for the telecommunications carrier are explicitly included in the carrier's license. Similarly, the license may specify rights to which the operator is entitled This licensing practice differs from that found in countries, such as the United States and Canada, where there has not been a

tradition of issuing licenses for certain telecommunications or information services. Instead, regulatory terms and conditions have traditionally been imposed on service providers through decision, orders or tariff approval processes of government regulatory authority rather than through the terms of an individual license. In Canada, therefore, quality of service standards and other matters would not be included in a telecommunications license and would instead be specified in ancillary decisions and orders of the regulator. The use of licenses that detail the specific rights and obligations of service providers may be desirable, however, in countries that lack clear or consistent regulatory policies or frameworks, or that have economic or governance problems. Countries that lack an established regulatory framework yet seek to facilitate growth of investment in communication, or information service providers may choose to issue licenses in order to provide sufficient regulatory certainty to these service providers. By specifying the rights and obligations of an ISP, a license may provide the relevant stakeholders—including the ISP, its investors, the government, and even consumers— with a clear understanding of what the ISP is, and is not, permitted or required to do during the term of its license. The clear definition of a communications provider's rights is often critical to enable the business to raise the financing needed to fund its operations and otherwise to operate its business. In the event that a licensing mechanism is adopted in an effort to protect ISP rights, regulators must ensure that any general authorization or individual licensing system is structured to provide for the lightest possible regulation of ISPs.

Best Practices for Licensing and Authorizations

Although licensing methods vary widely among countries, there are some common features that are considered to be among the best licensing practices. The following description draws largely upon practices advocated in the Licensing Directive adopted by the European Union in 1997, the General Agreement on Trade in Services (GATS) and the 1997 agreement on Basic Telecommunications of the WTO. While the European Union licensing directive is designed to govern procedures for authorizing telecommunications networks, may of its general principles also would be applicable to any licensing scheme adopted for ISPs. The recommended elements of an ISP licensing its authorization scheme are briefly listed below. These elements generally seek to ensure that any licensing or authorization requirements are open, non- discriminatory and transparent, and do not constitute unnecessary barriers to competition and innovation.

Best Practices for General Authorizations

The conditions for authorization are as follows:

i. conditions imposed on ISP authorizations should be nondiscriminatory, proportionate and transparent, and should be justified in relation to the service concerned. The specific types of conditions that may be permitted on general authorisations include;
ii. conditions intended to ensure compliance with relevant and essential requirements established by the regular;
iii. conditions linked to the provision of information reasonably required for the verification of compliance with applicable conditions and for statistical purposes;
iv. conditions relating to the protection of users and subscribers;
v. conditions relating to the interconnection of networks,
vi. conditions concerning ownership.

Notification

Service providers may be required to notify the regulator before providing the intended service. Service providers also may be required to provide information to the regulator to ensure compliance with any applicable conditions of operation. In such instance, the service provider may be required to wait for a reasonable and a defined period of time for example, up to four weeks, before starting to provide the services covered by general authorisation.

Right to Review, Remediation and Appeal

If the regulator finds that a service provider does not comply with the conditions of a general authorisation, it may inform the service provider that it is not entitled to use the general authorisation and/or impose on the service provider proportionate measures to ensure compliance. The service provider shall have an opportunity to state its views on the application of any such conditions and to remedy any breaches within a defined period of time. If the service provider is able to correct the breaches or deficiencies within a specified period of time, the regulator shall annul or modify its initial decision and state the reasons for this decision. If the service provider is unable to correct the deficiencies, the regulator shall, within a defined period of time, (for example, two months of its initial decision) confirm its decision and state the reasons for its decision. This subsequent decision shall be communicated to the service provider within a defined period of time, (for example, one week).-A procedure should also be established to permit the regulated entity to appeal the regulator's decisions to an independent

institution.

Best Practice Applicable to Licenses

Public Availability of Licensing Criteria

i. Where a license is required of ISPs, the following should be published and made publicly available;
ii. all licensing criteria;
iii. the period of time normally required to reach a decision concerning an application; and
iv. the terms and conditions of individual licenses;
v. The reasons for the denial of any license must be made known to-the applicant upon request.

• Licensing Conditions

Any license condition must be objectively justified, proportionate, non-discriminatory and transparent. See, for example, the allowable conditions for general authorisations described above. Regulators generally should keep license conditions and filing requirements to a minimum. It would be unduly burdensome, for example, to require ISPs to submit excessive amounts of business information to the regulator, such as: business plans; extensive technical filings; showings of experience; bank statements; or information detailing the source of funding.

•. Granting and Revoking Licenses

All licenses should be granted through open, non-discriminatory and transparent procedures. Furthermore, all applicants should be subject to the same procedures, unless there is an objective reason for differentiation. Any entity that fulfils the conditions adopted and published by the regulatory authority shall be entitled to receive an individual license. When a license fails to comply with a condition attached to the license, the regulatory authority may withdraw, amend, or suspend the individual license or impose, in a proportionate manner, specific measures aimed at ensuring compliance. The regulatory authority shall, at the same time, give the entity a reasonable opportunity to state its view on the application of the conditions and, except in the case of repeated breaches by the entity, the entity shall have an opportunity, within a defined period of time, to remedy the breach. If the breach is remedied, the regulatory authority shall, within a defined period of time, annul or modify its decision and state the reason for its decision. If the breach is not remedied, the regulatory authority shall, within a denned

period of time after its initial intervention, confirm its decision and state the reasons for its actions. The decision shall be communicated to the entity within a defined period of time that is, one week.

• Time Limits

The regulator should adopt and adhere to reasonable time limits for acting upon license requests.

• Artificial Barriers to Entry

The regulator should impose no artificial limits on the number of operators or service providers in the market. For example, since there is no network scarcity on a wire-line network compared with, for example, radio frequencies; there is no reason to restrict the number of ISP providers.

• Appeal

A procedure also should be initiated to permit an entity to appeal any decision by the regulatory authority to an independent institution.

Best Practices Applicable to both Licenses and Authorisations

• Public Consultation

To ensure fairness and transparency in the licensing or authorization process, the regulator should consult the industry, the public and other stakeholders.

• Fees

The fees associated with obtaining a license or authorization should not impose unnecessary costs on ISPs, and should not otherwise create a barrier to market entry. Therefore, to the extent that a regulator imposes fees on the issuance of a license or general authorization, the fees should seek to cover only the administrative costs incurred in the issuance, management, control and enforcement of the applicable authorization scheme. In addition, charges must be imposed in a non-discriminatory manner so that one operator is not charged more than another without some objective basis for so doing. Any fees also shall be published in an accessible and appropriately detailed manner.

Reference is made to the Internet Service Provider which facilitates the conduit of connections, which possibly results in an access through network connections, the copyrighted work stored on another's computer. Section 79 of the Information Technology (Amendment) Act, 2008 specifically deals and provides as follows: (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him. (corrected vide ITAA 2008) (2) The provisions of sub-section (1) shall apply

if- (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or (b) the intermediary does not- (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf (Inserted Vide ITAA 2008) (3) The provisions of sub-section (1) shall not apply if-

(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act (ITAA 2008) (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

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

Under the Australian statute of Copyright Act, 1968, Sections 36 and 101 provides that a person may be liable for authorizing the act which constitutes infringement and provides for 3 factors to be considered in determining whether the person authorized an infringement. The 3 factors are:

a. the extent of the person's power to prevent the doing of the act concerned;
b. the nature of any relationship existing between the person and the person who did the act concerned;
c. whether the person took any reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.

In view of the above provision, the website operator providing hyperlinks to other websites that allow infringing contents to be downloaded will be held liable[14] and the university facilitating photocopying in the library without giving any copyright warnings to users will also be liable.[15] Thus, the Australian law also provides for an incentive to the Internet Service

[14] Universal Music Australia Pty Ltd v Cooper [2005] FCA 972 at http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/federal_ct/2005/972.html?stem=0&synonyms=0&query=title%20(%20%22universal%2 0music%22%20); last seen on April 18, 2025
[15] University of New South Wales v Moorhouse [1975] HCA 26

Provider from the liability of contributory infringement, in cases where they have taken reasonable steps to avoid/prevent infringement. However, where Internet Service Provider fails to comply the reasonable steps and/or is found to authorize the infringement, then the right holder is available with the remedy of injunction and monetary relief. However, when the Internet Service Provider has complied with the safe harbor provisions such as no interfering in the downloads and access made by the user, taking reasonable steps to stop and from repeat of any copyright infringement, putting down the links of the website that provides downloads of infringing contents and materials, the remedies in these cases will be limited to non-monetary remedies.[16] Australia has through free trade agreements with countries like the United States, Singapore and Korea though not ratified, accepted the obligation to provide incentive to the ISPs while co-operating with the copyright holders in preventing infringement on the online platform. The Australian court in Roadshow Films Pty Ltd &Ors v iiNet Ltd[17] have held that iiNet which is the Internet Service Provider will not be held liable for their subscribers who are viewing and downloading contents, as in this case, iiNet could in no reasonable manner have stopped or deterred the infringers from infringing the copyright. Thus, the ISPs will not be liable for authorizing any act by the subscriber that infringes copyright.

The Internet Service Provider does not have any concrete power to prevent a person/subscriber/user from doing any act which amounts to infringement, but still there are a number of ways such as sending copyright warnings / notices to the subscribers and imposing penalty that can be adopted by the ISPs to discourage the rampant growth of infringement of copyrighted material on the internet.

Harmonization of schemes/ systems to deter infringement and the adoption thereof by Internet Service Provider from different countries.

Government of different countries must frame and adopt effective schemes or systems to be adopted and implemented by the Internet Service Providers as a way for discouraging and/or preventing the acts of infringement on the internet. Such schemes or arrangements should be of broad application and should not be a mechanism to give industryparticipants a competitive advantage or disadvantage or impose unreasonable costs. Further, while doing so the governments have to take into consideration the public interest. The schemes/ system which

[16] Jonathan Band & Matthew Schruers, Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act, 20 Cardozo Arts & Ent. L.J. [v] (2002).
[17] [2012] HCA 16

may be adopted must not be stringent and firm that would impose sanctions without sufficient/ reasonable cause or interrupt the subscriber's internet access.

Conclusion

The exponential rise of digital content consumption and the parallel increase in copyright infringement have necessitated a critical examination of the liability of Internet Service Providers (ISPs). Chapter 5 of this dissertation reveals that existing legal frameworks, both in India and globally, grapple with balancing the rights of copyright holders with the operational freedom and technical limitations of ISPs. While some jurisdictions like the United States have adopted a "safe harbour" model under the Digital Millennium Copyright Act (DMCA), the ambiguity and inconsistent enforcement of intermediary liability in India remains a major legal and policy challenge. The Indian approach, primarily guided by Section 79 of the Information Technology Act, 2000 and the Copyright Act, 1957, lacks precision in dealing with modern digital realities and emerging technologies. The chapter also highlights the tension between encouraging ISPs to self-regulate infringing content and avoiding punitive consequences for their voluntary content moderation. The comparative analysis reveals that a fault-based standard, such as the Cubby rule, has limitations when applied to intellectual property violations, where strict liability often prevails.

In essence, the legal regime governing ISP liability must evolve to recognize the nuanced role of intermediaries—not as mere conduits or publishers, but as dynamic platforms with varying levels of control and responsibility. A reformed legal structure must ensure that copyright protection is enforced without creating a chilling effect on innovation, freedom of expression, and internet accessibility.

Suggestions

- **Codification of a Tiered Liability Framework-** Indian law should adopt a tiered or graded liability model distinguishing between different types of intermediaries (e.g., mere conduits, hosting platforms, content-curating platforms) and their levels of involvement in content transmission or storage.
- **Strengthening and Clarifying the Safe Harbour Provisions-** Section 79 of the IT Act should be revised to explicitly include safe harbour protections in cases of copyright

infringement, provided intermediaries act expeditiously upon receiving actual knowledge or a takedown notice.

- **Mandatory Notice-and-Takedown Procedures-** Introduce a uniform, transparent, and accountable notice-and-takedown mechanism, modeled on global best practices, to ensure timely removal of infringing content while safeguarding against misuse.
- **Encouraging Voluntary Self-Regulation with Incentives-** ISPs should be encouraged to implement proactive content identification and filtering technologies, with legal incentives provided to those who adhere to voluntary codes of conduct or best practice guidelines.
- **Establishment of an Independent Digital Adjudicatory Authority-** A quasi-judicial body should be constituted to handle disputes related to online copyright infringement and intermediary liability, facilitating speedy resolution and reducing the burden on regular courts.
- **Balancing User Rights and Copyright Interests-** Any liability regime must be framed in a manner that upholds fundamental rights such as freedom of speech, privacy, and access to information, by providing adequate checks on over-removal or arbitrary censorship of content.
- **International Harmonization and Treaty Alignment-** India should harmonize its ISP liability standards with international treaties such as the WIPO Internet Treaties and align its enforcement models with jurisdictions that offer a balanced approach to copyright and intermediary accountability.