Educational Administration: Theory and Practice
2024, 30(5), 7377-7390
ISSN: 2148-2403
https://kuey.net/

Research Article

Examining The Role Of Internet Service Providers In Cyberspace: A Comparative Analysis Of The Current Legal Landscape In India And The USA

Dr. Amit Singh[1*], Nidhi Shanker[2]

[1*]Head & Dean, Department Of Law, MJP Rohilkhand University, Bareilly Email: Amit.Singh@Mjpru.Ac.In
[2]LL.M, NET Faculty Member, Department Of Law, MJP Rohilkhand University, Bareilly, Email: Nidhi121994@Gmail.Com

Citation: Dr. Amit Singh, Nidhi Shanker. (2024), Examining The Role Of Internet Service Providers In Cyberspace: A Comparative Analysis Of The Current Legal Landscape In India And The USA. Educational Administration: Theory and Practice, 30(5), 7377-7390
Doi: 10.53555/kuey.v30i5.4165

ARTICLE INFO

ABSTRACT

Since the invention of the internet, people have been able to interact, relate, and communicate in a virtual environment known as cyberspace. Data that can be published, used, and discarded online powers the cyberspace environment. An Internet Service Provider (ISP) is an enterprise that offers internet connection, commonly called as ISP. Access can be obtained by cable, wireless, and fiber-optic connections, among other methods offered by ISPs. Although ISPs can offer a wide range of additional services, their main offering is internet connection. These may consist of email access, tech support to their customers, etc. Since their early days of providing dial-up internet service, they have advanced significantly. And this drastic shift and advancement in technology is raising questions regarding security and accountability. The infrastructural network, the transport system, and the gateway of cyberspace are the ISPs. The need for procedures to verify and regulate the validity, security, and privacy of data increased with the development of the internet and digital consumption. Therefore, this paper attempts to analyze the role of ISPs in cyberspace and the extent of their liability where they can be held accountable. It also puts forth certain suggestions for better regulation of ISPs.

Keywords: Cyberspace, Digital, Internet Service Provider, Intermediary, Liability.

Introduction

The Internet is a global network of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to link devices worldwide. A wide range of electronic, wireless, and optical networking technologies connect the private, public, academic, corporate, and government networks in this network of networks, which spans local to global boundaries. Peer-to-peer (P2P) communication is a computing advancement that was progressively introduced and improved. Email, phone calls, file sharing, and the World Wide Web's (WWW) interconnected hypertext documents and applications are just a few of the many information resources and services available over the Internet.

An Internet service provider (ISP) is a company that links users to the Internet and offers related services like website development and hosting. An Internet service provider (ISP) possesses the necessary hardware and communication line connectivity to establish a presence on the Internet for the region they cater to. Delivering content to end users online involves a variety of intermediaries, since there will always be a series of intermediaries involved in making a work available over the Internet. When someone wants to start a website, they first need to create an account with a hosting company. After that, they can upload pages to their website, which is physically housed on the host's "server," which is essentially a very large hard drive that is directly connected to the Internet. The uploaded documents are immediately accessible to anybody with an Internet connection once they are stored on the server. Access to the Internet is then made available by an access provider. The transported content travels via the infrastructure of a network provider enroute from host to access provider to end user. This provider not only provides the necessary physical infrastructure for signal transportation, but also transmits and routes the content to the intended recipient. A single legal entity frequently offers the full range of these services. ISPs play a crucial role in the transmission or dissemination of content created by third parties, but they neither start nor participate in the choice to distribute any specific content. The two primary services offered by ISPs are:

a) Web site building and hosting, which is carried out by a company that offers management and space for personal or commercial websites; and
b) Access providing, which is carried out by a company that makes arrangements for a person or an organization to have access to the Internet.
'All the actors involved in an internet transaction have a real-world existence, and are located in one or more legal jurisdictions...it may be that the internet, rather than being unregulated, is in fact the most heavily regulated 'place' in the world.
Like all other nations, India is finding itself in a situation where legal frameworks that were reasonable prior to the internet's explosive growth are either proving to be insufficient or, in some cases, are being repurposed as blunt tools of state power. There is an urgent need for reforms in a number of areas related to internet usage from all angles, be it with regard to social media, OTT platforms, Telephone Tapping, Privacy issues etc. India's internet usage has skyrocketed in the last few years; about 10% of the population is now regarded as active internet users. By 2025, there will be one billion internet users in India. Although there is no doubt that the country as a whole benefit from the increased access to and use of online resources, there are still many issues that need to be resolved, such as inadequate infrastructure, skewed sex ratios among internet users, and lack of access in rural areas and above all the legal regulation of intermediaries who act as mediators and make these interactions possible and effective in digital world.
It would not be inappropriate to discuss how the use of IoT became essential during and after the pandemic, in areas such as healthcare, education, office work, and other areas where technology enabled the Covid-19 pandemic. In addition, during the past two years, issues with the legal framework controlling India's Internet ecosystem have drawn public attention, with the media concentrating primarily on issues of censorship and surveillance.

Expanding Horizons of Information Technology & Related Aspects:

Information technology has been defined as the "technology of production, storage and communication of information using computers and microelectronics"[i] or 'the development, implementation, and maintenance of computer hardware and software systems to organize and communicate information electronically'.
With a solid base of digital infrastructure and increased access to the internet thanks to the government's Digital India Program, India is now ready for the next stage of its development, which will involve creating enormous economic value and empowering its people as more and more sectors adopt new digital applications. Nowadays, a large number of the largest corporations on the planet act as online information brokers. Facebook facilitates the sharing of information between its 1.5 billion users. Google acts as a middleman for users conducting over three billion searches daily on the internet[ii]. Among the world's top 17 economies, India's is currently the fastest-digitizing economy, with the potential to generate up to $1 trillion in economic value by 2025.
National scaling of thirty digital themes can expedite advancement in nine priority areas. The productivity and output of India's future digital economy could support between 55 and 60 million workers by 2025.[iii] "India is poised to be a trillion-dollar digital economy and could support 60 to 65 million digitally enabled jobs by 2025-26".[iv] To develop the future work force in emerging digital skills, MeitY and NASSCOM have jointly initiated a programme titled "Future Skills PRIME (Programme for Re-skilling/Up-skilling of IT Manpower for Employability)" which aims to create a re-skilling/up- skilling ecosystem in futuristic technologies.
Among the initiatives offered by Digital India are Diksha, eNAM, eSanjeevani, and DigiBunai. Important technological advancements made in India include the Unified Payments Interface (UPI), e-KYC, and the JAM trinity, which consists of Jan Dhan, Aadhar, and mobile. According to CERT-In, there were 14,02,809 and 6,74,021 cyber security incidents in total that were noted in 2021 and 2022 (up until June), respectively. In contrast, a study carried out in the last few months by the Cyber Peace Foundation, a civil society organization, Autobot infosec, and Cyberspace Center of excellence, found that 3.6 lakh cyberattacks were directed towards Indian oil companies. In order to publish research on the regulation of social media intermediaries, online news media, and OTT platforms in seven different countries worldwide in 2022, OPBP teamed up with the IFF, a nonprofit organization dedicated to digital rights that operates in India. As established by a number of significant metrics, from Internet connections to mobile application downloads both the volume and the growth of India's digital economy now exceeds that of most other countries. According to a report, "the number of active internet users in India is expected to increase by 45% in the next few years and touch 900 million by 2025 from around 622 million in 2020".[v]
Digital services are being rapidly adopted on social media platforms, communication platforms, services platforms, OTT platforms, and online news platforms due to the growing demand for remote work and infotainment. 63% of Indians reported using social media to get news, compared to 59% for TV, 49% for print media, 53% for YouTube, and 51% for WhatsApp, according to the Digital News report 2022 from the UK-based Reuters Institute for the Study of Journalism. The needs of the user base—video conferencing and group voice calling, for instance—have quickly evolved from being convenience-enabling services to everyday necessities in the new post-pandemic normal. In the coming years, India's OTT Video services are predicted to grow to be a Rs 21,031 crore industry by 2026, with Rs 19,973 crore coming from subscription-based services and Rs 1,058 crore from transactional VOD (video on demand), according to PwC's Global Entertainment & Media Outlook 2022-2026.In addition to offering chances for expansion and development, the changing digital

economy presents a possible location for traditional regulatory mechanisms to be reoriented in order to maintain policy relevance and foster innovation. In 2020, NASSCOM released a research paper titled- 'The New Decade Strategic Review' which highlighted the need to integrate rapidly evolving Technology with people's lives to bring in change. “The Indian media and entertainment industry is one of the fastest growing media industries in the world and is projected to reach USD 100 billion by 2030”.[vi]

Information Technology in India: -

India established its first electronic commerce law, the Electronic Commerce Act, 1998, together with the Electronic Commerce Support Act, 1998, in response to the aforementioned initiative. The shift from paper-based to electronic transactions raised concerns about the legitimacy, enforceability, and recognition of electronic documents and signatures. Additionally, legislators faced the difficult task of reconciling the competing interests of promoting technological advancement and preserving electronic commerce. The 1998 Draft of the Electronic Commerce Act by establishing a legal framework governing electronic contracting, the security and integrity of electronic transactions, the use of digital signatures, and other matters pertaining to electronic commerce sought to "facilitate the development of a secure regulatory environment for electronic commerce."[vii].

Eight parts of a different draft, dubbed the Electronic Commerce Support Act, 1998, focused mostly on what needed to be changed to other Acts in order to completely harmonize them with the Electronic Commerce Act of 1998. The Information Technology Bill, 1999 emerged with the establishment of the Ministry of Information Technology. In December 1999, the Bill was presented to Parliament, and on May 9, 2000, it was approved by the President. It became operative on October 23, 2000.

Information Technology Act, 2000:

In order to facilitate the electronic filing of documents with government agencies, the information technology Act of 2000 sought to give legal recognition for transactions conducted through electronic data exchange and other means of electronic communication, also known as "Electronic Commerce." This type of commerce involves the use of alternatives to paper methods of communication and information storage. In order to do this, amendments to the “Reserve Bank of India Act 1934, the Indian Evidence Act 1872, the Indian Penal Code 1860, and the Banker's Books Act 1891” were also required. The Act included four schedules, thirteen chapters, and ninety-four sections. There are provisions on digital signatures, e-governance, intermediates, certifying authorities, electronic signature certificates, offenses and associated fines, etc. As against the parent Act, The Act extends to the whole of India and, in some cases, even outside India. Following the passage of Negotiable Instruments Amendment Act 2002, the IT Act 2000 underwent some major changes with effect from February 6, 2003.

The Act incorporates the following objectives:

1. To legally recognize any transaction that is being done by e-commerce, other electronic means of communication, or data interchange in lieu of the previous communication method that is based on paper work.
2. To give “legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication”.
3. “To facilitate the electronic filing of documents with Government agencies and also departments.”
4. To Facilitate the electronic storage of data.
5. To Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions.
6. To Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Features of the Information Technology Act, 2000:

1. Legal validity exists for all electronic contracts executed over secure electronic means.
2. Acceptance of digital signatures by law. Digital signatures and electronic records are protected by security protocols.
3. A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized.
4. The IT Act makes provision for the creation of a Cyber Regulatory Appellant Tribunal. This tribunal will hear appeals against the Controller or adjudicating officer orders.
5. Only the High Court will accept an appeal against the Cyber Appellant Tribunal's ruling.
6. A hash function and an asymmetric cryptosystem will be used in digital signatures.
7. Additionally, there is a provision for the Controller of Certifying Authorities (CCA) to be appointed in order to license and oversee the operations of Certifying Authorities. All digital signatures will be kept in one repository by the Controller.
8. The IT Act also applies to contraventions or offences committed outside India.
9. The Act includes provision establishing a Cyber Regulations Advisory Committee to provide guidance to the Controller and Central Government.

IT Act with rules 2009:

"Section 69 of the IT Act and the **Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009"** are the relevant laws under the IT Act that governs the cyberspace and transactions that are being carried on in this virtual space.

In the interests of" India's sovereignty and integrity, defense, security, friendly relations with other countries, public order," preventing the incitement to commit any cognizable offense related to the aforementioned, and for the purpose of an investigation into an offense, Section 69 of the IT Act permits the interception, monitoring, and decryption of digital information. Its scope is twofold more than that of Section 5 of the Telegraph Act.

There is apparent lack of the necessity to meet public safety or emergency situations in Section 69 of the IT Act.

The detailed procedure is given in "Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 which, inter alia, provides the following safeguards:

1. Recording of reasons for interception of any information.
2. Direction for interception shall not exceed 60 days from the date of its issue. It could be further renewed but the period shall not exceed the total period of 180 days.
3. Destruction of records of information obtained from such interception with 6 months unless such information is required for functional needs.
4. There is a confidentiality obligation on the intermediaries not to disclose any information obtained related to third-party".[viii]

On the other hand, Pegasus spyware involves the deployment of spyware to breach the nation's mobile phone users' privacy. Section 43 of the Information Technology Act prohibits anyone from hacking a mobile phone without the owner's consent. Individuals found guilty of dishonestly or fraudulently hacking a mobile phone face up to three years in prison, a fine of up to five lakh rupees, or both under Section 66 of the IT Act.

Government of India (Allocation of business Rules, 1961):

The Ministry of Electronics and Information Technology in India is empowered to create and regulate anything related to the Internet and technology, according to the Government of India (Allocation of Business Rules, 1961).[ix]

Telecom Regulatory Authority of India Act 1997:

The TRAI Act of 1997 created the Telecom Regulatory Authority of India (TRAI) on February 20th, with the goals of regulating telecommunication services, resolving disputes, handling appeals, safeguarding the interests of telecom service providers and customers, and fostering the expansion of the telecom industry.

At a meeting in the Lok Sabha on September 16, 2020, the Minister of State for Communications, Education, and Electronics and Information Technology informed the members of Parliament that the Telecom Regulatory Authority of India ("TRAI") had released its recommendations for the Department of Telecommunications ("DOT") to regulate Over-the-Top ("OTT") Communication Services[x].

The "Telecom Tariff (66th Amendment) Order, 2022 (1 of 2022)" was released by TRAI on January 27, 2022. The Authority has received references from customers who are unhappy that telecom service providers (TSPs) are only offering tariffs with a 28-day validity period (or multiples of 28 days) as opposed to 30-day tariff options. The Authority has observed, however, that TSPs have not tried to promote the same as monthly tariffs and have been open about the validity duration of the aforementioned tariff offers, which is 28 days, etc.

1. Accordingly, as per extant practice, a Consultation Paper on "Validity period of Tariff Offers" was issued by the Authority on 13.05.2021, seeking comments and counter comments from stakeholders.
2. Following subclause (x) in clause 6 of the Telecommunication Tariff Order, 1999, the Authority has decided to insert subclauses (xi) and (xii), after taking into account the opinions of all stakeholders and participants and analyzing worldwide practice in this regard, which were as follows: (xi) With a thirty-day validity period, each telecom service provider must provide a minimum of one Plan Voucher, one Special Tariff Voucher, and one Combo Voucher. (xii) It is required that each Telecom Service Provider provide a minimum of one Plan Voucher, one Special Tariff Voucher, and one Combo Voucher. These vouchers must be renewable on the same date each month.
3. Telecom customers would have additional options to select service offers with the right validity and duration if the amendment is enacted. The cases of **Reliance Jio Infocom Ltd vs Vodafone- Idea Ltd & Others (2022)[xi], Vodafone Idea Ltd vs Union of India (2021)[xii]** are some of the recent controversies which brought into news the Abovementioned Act and Tribunal (TDSAT) established therein.

Indian Cinematograph Act, 1952:

The Indian Cinematograph Act of 1952 instituted censorship to seemingly protect audiences from the immorality ideals portrayed in the films. The Act set up a Central Board of Film Certification ("CBFC"), which is responsible for regulating the public exhibition of films in India. It certifies and classifies the films in the following categories[xiii]:

- 'U' "(unrestricted exhibition)
- 'UA' (unrestricted exhibition except for children below 12 years of age)

- 'A' (restricted to adults only) and
- 'S' (restricted to a specified class of persons)"[xiv]

The point of concern is whether the OTT platforms which are also considered as intermediaries will be covered under the Indian Cinematograph Act, 1952 as it applies to cinematographic films. Thus, it whether a film is being published theatrically or over on OTT platform, it needs to have a certification of Central Board of Film Certification. There is no settled rule as to responsibility and liability on the part of OTT platforms in case there is violation of any of the provisions of the said Act and also what shall be extent of the application of the said Act on the intermediaries.

The draft Indian Telecommunication Bill, 2022

The Bill seeks to replace the existing legal framework comprising the "India Telegraph Act 1885, the Wireless Telegraphy Act 1933 and the Telegraph wires (unlawful possession) Act, 1950" that currently govern the telecom sector.

The purpose of the bill is to update and combine the current legislation pertaining to the establishment, growth, and operation of telecommunications services.

Key Provisions

- The Bill proposes amendments to the TRAI Act, 1997.
- According to the Bill, a user who receives a message sent using telecom services will be able to identify the sender.
- The definition of Telecommunication services is widened & covers OTT platforms, whatsapp, zoom, netflix etc.
- Information received or transmitted "could be intercepted by authorized official of the government in the interest of sovereignty integrity or security of India".[xv]

Concluding analysis:

The Information Technology Act of 2000 (IT Act) is the primary legislation in the contours of cyberspace in India. As the OTT, television and other mass media industries, streams a variety of content across the internet, there is a presumption that this legislation is exclusively applicable to it. However, the IT Act does not apply to all the facets of the video streaming OTT platforms etc. It is only applicable to statutory offenses and does not regulate the content as the CBFC or IBF does.

To understand the application of the statute on digital content, it is essential to understand the concept of intermediaries under the IT. An intermediary is a crucial link to the internet as it distributes, publishes, or transmits information and creates an 'interactive' world.

Defining Intermediary-

An intermediary has been defined in Sec. 2(1)(w) of the Act[xvi], as "any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record & includes telecom service providers, web housing service providers, search engines, online payment sites, online auction sites, online market places & cyber cafes".

Intermediaries carry out a wide range of tasks, but typical ones include content hosting, information gathering, information evaluation, communication and information exchange facilitation, information aggregation, internet access, etc. Intermediaries include cloud service providers, cyber cafes, social media sites, search engines, and ISPs.

Statutory Framework Under I.T. Act, 2000 regarding Intermediaries: -

A safe harbor provision found in Section 79 of the Act shields intermediaries from liability for the actions of third parties under certain conditions. Section 79(1) of the Act gives intermediaries this protection with regard to any information, data, or communication link that they host or make available to third parties. The Act's Sections 79(1) and 79(3) apply to this immunity.

In essence, situations where the intermediary engages in technical, automatic, or passive activities are covered by Sec. 79(2). Therefore, in order for Section 79(1) to be relevant, intermediaries must not be aware of or in charge of the information that is transferred or stored.

Moreover, Sec. 79(3)(6) envisions a "notice and take down" system in which the intermediary must remove illegal content as soon as it becomes known to exist.

In "**Shreya Singhal v/s UOI,"** the Supreme Court read down Sec. 79(3)(6) to mean that an "intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts related to Art. 19(2) are going to be committed then fails to expeditiously remove or disable access to such material."

As a result, an intermediary need only take action in response to a notification from the relevant government body or court order. Regarding the content that needs to be disabled or removed, the intermediary is not obliged to use its own judgment.

Hence, Section 79 limits the exemptions granted to only such intermediaries who do not aid, abet or induce the authorities prohibited under the law. This statutory provision appears to be a safe Harbor clause based on

the European directives.[xvii] This provision is also similar to that of the US Laws[xviii] intermediaries. However, the safe harbor protection under Indian law is available only to 'passive intermediaries', those who 'acts as conduits or passive transmitters of the records or information.[xix]
There are several rules made governing norms regarding intermediaries, online content, etc. which are discussed as follows:

The IT (Procedure for Interception etc. of Information) Rules, 2009: -
☐ **Intermediary to provide facilities (v-13)**. Along with requesting in writing that the designated officers of the intermediary or person in charge of the computer sources provide all facilities, cooperation, and assistance for the interception, monitoring, or decryption mentioned in the directions, the officer issuing the requisition conveying the directions issued under rule 3 for information interception, monitoring, or decryption.
☐ **Intermediary to designate officers to receive and handle requisition (v-14)** Every intermediary in control of a computer resource must designate one officer to accept requests for information generated, sent, received, or stored in any computer resource, and another officer to handle requests for information from the nodal officers regarding interception, monitoring, or decryption.
☐ **Intermediary to ensure effective check in decryption of Information (R.19-20)** R. 19 states that, in the event that the agency requests it, the intermediary or the person in charge of the computer resource so directed (under R. 3) shall offer technical assistance and the equipment, including hardware, software, interface, and access to the equipment, and be authorized to perform interception, monitoring, or decryption, including for the purposes of (i) installation, (ii) maintenance & (iii) removal of such equipment and the performance of any action required for accessing stored information under the directive issued by the competent authority (under R. 3).
In contrast, R. 20 requires the intermediary or person in charge of computer resources to set up a sufficient and efficient internal check on the unauthorized interception of information, to guarantee the preservation of confidentiality, and to take the highest care and precautions when it comes to monitoring, decrypting, or intercepting information.

- **R. 21 (Responsibility of Intermediary)** If an employee violates any laws pertaining to maintaining the confidentiality and secrecy of information, or if there is any unauthorized monitoring, decryption, or interception of information, the intermediary or person in charge of computer resources will be held accountable for any actions taken in accordance with the applicable laws currently in effect.

The IT (Procedure & Safeguard for Blocking of Information) Rules, 2009:
In response to growing concerns about China, the Ministry of Electronics & IT of the Government of India blocked 118 mobile apps that were detrimental to public order, security of the state, Indian sovereignty and integrity, and defense by using section 69A of the Information Technology Act and relevant provisions of the "Information Technology (Procedure & Safeguards for Blocking of Access of Information by Public) Rules, 2009."

R.5 Intermediary to ensure effective check in handling of traffic data or information: The intermediary or person in charge of computer resources must implement sufficient and efficient interval checks to guarantee that there is no unauthorized monitoring or collection of traffic data or information, that extreme secrecy is maintained, that the matter of monitoring or collecting traffic data or information as it affects citizens' privacy is handled with the utmost care and precautions, and that this matter is handled exclusively by the designated citizens and the designated officer of the intermediary or person in charge of computer resources.

The IT Intermediaries (Guidelines) Rules, 2011:
The rules were introduced by the Central Government in exercise of powers under S. 87(2) (2g) read with S. 79(2) of the Information Technology Act, 2000.

R. 3 (Due diligence to be observed by intermediary): "The intermediary shall publish the rules and regulations, privacy policy & user agreement for access or usage of his computer resource by any person. By so doing the intermediary shall inform the users of his computer resource not to host, display, upload, modify, publish transmit, update or share any information that-
(a) Belongs to another person and to which the user does not have any right to; or
(b) is grossly harmful, harassing, blasphemous, defamatory obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful or racially or ethnically objectionable, disparaging, relating or encouraging money laundering or gambling or otherwise unlawful in any manner whatever; or
(c) harms minor in any way; or
(d) infringes any patent, trademark, copyright or other proprietary rights, or
(e) violates any law for the time being in force; or

(f) deceives or misleads the addressee about the origin of such messages or communications any information which is grossly offensive or menacing in nature; or
(g) impersonates another person; or
(h) contains software issues or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource; or
(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes, incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation".
The Information Technology (Reasonable Security Practices & Procedures & Sensitive Personal Information) Rules, 2011 stipulate that the intermediary must take all reasonable steps to secure its computer resource and the information contained therein.
He will notify the Indian Computer Emergency Response Team of cyber security issues and share information pertaining to cyber security occurrences with them.

In "Shreya Singhal v/s Union of India"[xx]: Rule 3(4) of the 2011 rules was read down to the extent that an intermediary would only be required to disable information that would be relatable to article 19(2) of Indian Constitution.

"Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" -
The rules 2021 have been framed in exercise of powers under section 69A (2), 79(2)(c) & 87 of the IT Act 2000 & therefore the Information Technology Act (Intermediary Guidelines) Rules 2011 stands replaced

Reasons for the need of rules:
The Digital India initiative has evolved into a movement that uses technology to give average Indians more influence. The widespread use of mobile phones, the internet, and other technology has also made it possible for numerous social media platforms to grow in India. These platforms are also being heavily utilized by regular individuals.
Furthermore, India moved up 37 spots to rank as the tenth best country in the world on critical cyber safety parameters according to the International Telecommunication Union's 2020 Global Cyber Security report, which was announced. The US, topped the chart, followed by UK & Saudi Arabia tied on the second position while Estonia was ranked third in the index.[xxi]
However, the continual dissemination of false information has forced numerous media outlets to establish fact-checking procedures. Rampant use of social media, misuse of social media for setting corporate rivalries in blatantly unethical manner, prevalence of child pornography[xxii], lack of transparency & accountability of digital platforms has become a major concern for businesses.
In addition, a strong complaint system is required, allowing regular users of social media and over-the-top (OTT) platforms to file complaints and receive prompt resolutions.

Rationale and Justification for New Guidelines:
The Supreme Court in Suo moto writ petition (Prajawala)[xxiii] case vide order dated 11.12.2018 had observed that Govt. of India may frame necessary guidelines to eliminate child pornography and videos and sites in content hosting platforms of their applications.
The Supreme Court vide order dated 24/09/2019[xxiv] had directed the Ministry of Electronics & IT to apprise the timeline in respect of completing the process notifying the new rules.

Categorization of Social Media Intermediaries:
(a) Social Media intermediaries (includes all intermediaries) - Rules
1. Due diligence shall be followed by intermediaries
2. Intermediaries must set up grievance redressal mechanism
3. Intermediaries must ensure online safety and dignity of users, specifically women users
- After receiving complaints, intermediaries have 24 hours to disable or remove access.
4. Intermediaries must bring voluntary user verification mechanism
- Visible mark of verification
5. Intermediaries must remove unlawful information
- Platforms should not host or publish any information that is forbidden after obtaining real knowledge in the form of a court order or notification from the relevant government agency.
6. Rules shall come in effect in 3 months after publication of these rules.

According to Rule 2(w), a social media intermediary is an intermediary that primarily or exclusively permits users to communicate online and to produce, post, and distribute content through its services.

(b) Significant Social Media Intermediary:

Significant social media intermediary means having registered users above the threshold as notified by the government.
Release a monthly compliance report that includes information about the items that the major social media intermediary has taken proactive measures to delete, as well as the specifics of complaints received and the steps taken in response to them.
Significant social media intermediaries that offer services mostly related to message must make it possible to identify the original source of the content.
The intermediary is not obligated to reveal the message's content or any other information belonging to the original author**.**

However, the Proposed changes suffer from Infirmities which are set out below:

(1)Legal Aspect:

After a thorough analysis of the regulations, it may be concluded that determining the message's original source would take precedence over end-to-end encryption guidelines or different social media middlemen:

1. The policy of tracing a message's initial source can be unduly misused against any individual, even though it would aid in identifying the primary offender in the event of an offense.
2. In addition, people would be unwilling to voice their opinions, which would ultimately impede the free exchange of information and deny the populace their fundamental right to freedom of speech and expression (Article 19(1)(a) of the Indian Constitution).
3. Additionally, the rules have an overly broad delegation of authority because they provide a non-judicial adjudicatory process for complaints about content that is published by OTTs and Digital News Media.
4. Creation of 'oversight committee'.
5. 'Flawed consultation' is the main drawback while regulating he online news portals and video streaming platforms.
6. "While examining the 2011 Rules on intermediary guidelines, the Lok Sabha Committee on subordinate legislation (2013) had observed that to remove any ambiguity, the definitions of the grounds used in the rules should be incorporated in the rules, if the definitions exist in other laws."[xxv]

(2) Political Aspect:

1. The exclusion of speeches and information opposed to government authorities may contravene the provisions as under Right to Information Act, 2005 as well.
2. The very purpose of freedom of speech and expression would be defeated, in case the discretionary powers are blatantly misused.

(3) Social Aspect

1. In digital era, though public needs a platform which discuses socio-political issued irrespective of any bias, and in order to provide real information and prevent spread of fake news curbs are required to be imposed, but regulation of content should not be in derogation of citizens right to privacy as under Article 21of Indian Constitution.
2. Tracking first originator will harm transparent communication, it may serve as intrusion into individual privacy.
3. The content takedown timeline is thereby six hours. The intermediaries should answer the request from a law enforcement agency regarding unlawful content within seventy two hours. But in most cases, the intermediaries do not have sufficient information to respond within that given timeline. There are situations where the organization cannot meet the timelines because of unavailability of data in that aspect, it requires more clarifications.
4. Enabling Traceability will lead to retention of more personal data by messaging services which goes against the principle of data minimization.[xxvi]

(4) Other Aspects:

Rule 4(a) mandates the significant social media intermediaries to appoint a chief compliance officer a nodal contact person, a resident grievance officer. All the three should be a:

1. Resident of India, which creates hardships for multinational companies.
2. The requirement of a local office also creates a burden for international companies.
3. Lack of digital literacy also can be misused.
4. Right to privacy is also declared as a fundamental Right under article 21 of India Constitution by Hon'ble Supreme Court in J.K.S. **Puttaswamy & Anr. v/s Union of India**[xxvii]. It was also observed by the Apex Court that right to privacy is not an absolute right and any invasion of privacy by state or non-state actor must satisfy the triple test i.e. (a) Legitimate Aim
(b) Proportionality
(c) Legality

Judicial Approach:

1. Avanish Bajaj v/s State (NCT) of Delhi (Bazee com Case)[xxviii] There is no threshold for holding intermediaries principally accountable for the content, which could result in earlier criminal penalties, when they are found guilty under section 79 for breach of safe harbor or for liability under the copyright Act.

2. Snapdeal Private Limited v/s Godaddy.com Inc and Others.[xxix] The Delhi High Court has held that the Domain name registrars are "Intermediaries", within the meaning of Sec. 2(1)(w) of the Information Technology Act, 2000.
"As being persons who provides service with respect to the domain names, the domain name registrars would be "intermediaries" within the meaning of Section 2(1)(w)," the court held.
Furthermore, the court stated that the functions that an intermediary can undertake are not defined or limited by the IT Act or the 2021 IT Rules.

3. My Space Inc. v/s Super Cassettes Industries Ltd. (2016)[xxx] In this instance, Super Cassettes India Ltd. sued myspace.com, claiming that the website permits users to distribute Super Cassettes' copyrighted content without authorization. The court ruled that the harmonious reading of Sections 51(a)(ii) of the Copyright Act and Sections 79 and 81 of the IT Act is required. The intermediaries may be held accountable if they have actual or specific knowledge that there is illegal content on their website and they choose not to remove it in spite of being notified of this fact, according to the court's introduction of the notion of "actual or specific knowledge."

4. Google India Private Ltd. v/s Vishakha Industries and Another [xxxi] The Apex Court held that there is no protection for intermediary under Sec. 79 of IT Act from Criminal defamation before 2009 amendment.
It was held that before the amendment made to Section 79 of the Information Technology Act in 2009, a network service provider was protected only from liability under the IT Act. The protection did not extend to liabilities arising under other enactments, prior to 2009 amendments. On this reasoning, it was held that Google India could not claim immunity from liability for criminal defamation under Section 499 of the Indian Penal Code, in a complaint which arose before the 2009 amendment.

5. Christian Louboutin SAS v/s Nakul Bajaj and Others. (2018)[xxxii] In this case, Delhi High Court had to decide on the liability of an e-commerce platform, darveys.com for infringement of trademark rights of Christmas Louboulin whose products were being sold on the platform.
The court distinguished 'active' and 'passive' intermediaries and held that Sec. 79 of the IT Act is to protect genuine intermediaries and cannot be abused by extending it to those people who are not intermediaries and are active participants in unlawful act. The court also laid down certain factors to identify an active intermediary, namely identification of the seller and providing details of the seller, providing quality assurance, authenticity guarantees or storage facilities; assistance for placing a looking of the product; creating a listing of the product; packaging of the product with its own packing; transportation; delivery; and advertising products on the platform etc. If a large number of elements enumerated above are present, then such intermediary shall be deemed to be an active participant and would not be exempted under Section 79 of the IT Act.

6. Amazon Seller Services Pvt. Ltd. v/s Amway India Enterprises Pvt. Ltd. and Others. (2020)[xxxiii] In this historic case, the Delhi High Court ruled that an intermediary shall not be liable for any third-party information, data, or communication link made available or posted by it, provided that the intermediary complies with sections 79(2) or (3) of the IT Act. The court further held that there is no distinction between passive and active intermediaries with regard to the availability of the safe harbors provision.

7. Shreya Singhal v/s Union of India (2015)[xxxiv] The Hon'ble Supreme Court invalidated Section 66A of the IT Act 2000 in this historic decision, finding that it violated Article 19(1)(a) of the Indian Constitution. In this instance, the IT Act's Section 79(3)(b) was also contested, arguing that it extends the definition of "unlawful acts" beyond the topics covered by Article 19(2) of the Constitution and permits the intermediary to use its own discretion upon learning that any information is being used to commit crimes. The Supreme Court interpreted Section 79(3)(b) to mean that the intermediary shall promptly deny or disable access to such content upon realizing that a court order has been issued. This interpretation upholds the constitutionality of the original provision. Second, the government's notice or the court order must adhere to the provisions outlined in Article 19(2).
The current scenario is that there is still lack of a comprehensive law regulating Internet Service Providers. Some aspects have developed through case laws while others have been formulated through rules formed incidental to the main statute primarily which is Information Technology law in India. Although "intermediary" is defined under IT Act, still it is subject to interpretation by courts in different situations such as in the case of Snapdeal Private Limited v/s Godaddy.com Inc and Others, where the question was whether "Domain name Registrars" will fall under the definition of intermediary or not. Thus, there is need to further develop the law on this subject matter comprehensively.

Copyright Act & Rules Amendments:

- Provide for safe harbour for intermediaries under Section 51(a)(ii).
- The liability regimes under Section 79 of the IT Act and Section 51(a)(ii) of the Copyright Act may be harmonized.
- Section 52(b) and (c) of the Copyright Act as well as Rule 75 of the Copyright rules may be amended to require judicially determined orders for content restriction.[xxxv]

In this case, before the enactment of safe harbor under section 79, the court found the proprietor of a website criminally liable for content hosted on its marketplace.

Intermediary Rules & Digital News - Recent Developments:

It has been confirmed by Ministry of Information & Broadcasting on May 26, 2021 that digital news publishers fall under the applicability of intermediary Rules to digital news platforms is due to following reasons:
The Code of Ethics under the intermediary Rules (Code of Ethics) mandates that the digital news publishers shall adhere to the (a) Programme Code under the Cable Television Networks (Regulations) Act, 1996 (b) Norms of Journalistic Conduct under the Press council Act 1978; and prohibitions of publications of content prohibited under any other law in force at the time.
While the Press Council Act and the Press & Registration of Books Act 1867 covers e-versions of newspapers, the news portals & news websites are not covered under the Press Council Act.
Similarly, while the cable T.V. Act and up linking and down linking guidelines for Private T.V. Channels, 2011 cover TV news entities, they do not cover digital portals of such entities.[xxxvi]
However, in a case, decided by Bombay High Court, it was observed that Intermediary Rules go beyond the scope of IT Act, which was not passed for Regulations of news media. S.87 of the IT Act which mandates that Central Govt. may create required rules under the IT Act sets out very detailed instances for which the Central Government may create rules and clearly does not include formulations of rules which would regulate digital news media.

Proposed Changes (2022) to IT Rules, 2021:

In February, 2021 under the IT Act, 2000, M city issued the IT Rules, 2021 which finalized the draft IT Rules of 2018 and superseded the earlier IT Rules of 2016 & 2011.[xxxvii]
Subsequently in June 2022, MeitY released the proposed draft amendments to the IT Rules 2021.

1. Shorter timeline in dealing with user grievances: An intermediary would have to acknowledge a complaint received from a user by its Grievance Officer (GO) within 24 hours & respond to requests for removal within 72 hours.

2. Opportunity to dispute actions taken by platforms: The draft proposed that a user should be provided an opportunity to dispute any action taken by an intermediary, including asking for reinstatement of any content that is taken down.

3. Provisions for a Grievance Appellate Committee: According to the amendment, the Central Government would have constituted one or more Grievance Appellate Committees. These would comprise of: "A Chairperson, such other Members, as the Central Government may, by notification in the Official Gazette, appoint".

4. Expectations of transparency, respecting constitutional rights: The intermediary shall respect the rights accorded to the citizens under the Constitution of India.

5. Ensuring compliance with the privacy policy and other terms: The 2022 amendment proposed that after publishing their regulations, privacy policy and user agreement, an intermediary would also have to ensure user compliance with the same.

Provisions concerning ISPs in USA

There are basically two approaches adopted globally for governing ISPs. The first one being, horizontal approach, this determines ISP responsibility in a single location under a single statute. There are currently regulations in place in Germany, Sweden, Japan, and other countries that take a horizontal approach to the problem.

The possible liability of ISPs is ascertained under each applicable law in the non-horizontal method. ISP liability in this situation would be determined by a number of legislations; for instance, the copyright statute's non-horizontal approach would address ISP liability that might solely be related to copyright offenses. The United States of America, Singapore, Hungary, and Ireland have all chosen the alternative strategy of enacting copyright-specific laws to establish internet ISP responsibility.

Since the early 1990s, there has been discussion about ISP liability for illegal activities on the Internet. This topic has drawn attention from a number of US court cases as well as from ISPs' vigorous lobbying to limit their liability while changing copyright laws.

Any violation of the exclusive rights provided by the Copyright Act constitutes infringement. A two-prong approach has been adopted by courts across several nations, including the US and India, to evaluate if copyright infringement has occurred. First, if a legitimate copyright is identified, further investigation is done to determine whether any of the original work's component parts have been copied.

The United States of America amended its Copyright Act in October 1998 by passing the Digital Millennium Copyright Act (DMCA), which adds a new section 512 to chapter 5 of the US Copyright Act, with the goal of limiting the liability of ISPs. It creates "safe harbours" to protect Internet service providers from lawsuits alleging copyright violations under specific conditions.

Section 512(a) of the DMCA provides protection for the conduit function, which allows ISPs to transmit, route, or provide connections for material through a system or network that is controlled or operated by the service provider. These are the four main provisions of the DMCA that address the various functions of an ISP. Section 512(b) restricts an ISP's liability for caching, Section 512(c) safeguards content stored on the provider's system or network at the user's request, and, in certain cases, ISPs that offer information location tools like links or directories are also protected.

Even with the many regulations that safeguard intellectual property, it is still very difficult to keep an eye out for copyright violators on the Internet. A large number of lobbying groups, particularly those involved in the US music industry, supported making ISPs accountable for users' copyright violations. It is imperative to acknowledge that there exists a fundamental distinction between internet services that facilitate the transfer of content and those that provide the content themselves. While it seems sense to hold ISPs accountable in the latter case, it is obviously unjust to hold ISPs accountable for the infringements committed by their users. If ISPs are directly involved in the copying of content that is protected, they will be held accountable for copyright infringement. For instance, an Internet service provider would violate copyright if it allowed users to download unlawful copies of the newest songs from its website. ISPs are typically allowed to shut down websites and email addresses in the event of infringement under contracts they enter into with their clients, which is one of the key reasons for including them in the process and holding them accountable. They also offer hotlines for reporting abuse so that appropriate action can be taken.

Another provision concerning ISPs is provided under The Communications Decency Act, 1996. "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider," according to Section 230 of the Communications Decency Act, which was passed into law in the United States in 1996. As a result, it shields interactive service providers from legal action under local intellectual property regulations. This clause makes it impossible to hold ISPs accountable for their decisions to publish, remove, or modify content. Like the DMCA protections that shield ISPs from third-party copyright infringement, this provision was introduced because it would be unjust to hold ISPs accountable for the activities of others and would have a negative impact on free speech. Furthermore, as previously stated in this study, ISPs are unable to keep an eye on the hazardous information. However, in Chicago Lawyers' Committee for Civil Rights under the Law Inc. v Craigslist Inc[xxxviii], According to the Court's ruling, ISPs are shielded from liability as publishers for content created by third parties by Section 230(c)(1) of the Communications Decency Act. However, this immunity does not apply to all claims resulting from an ISP's provision of public access to such content. As a result, it is evident that the immunity granted to ISPs has restrictions and that they are not always immune from punishment.

Conclusion

The in-depth analysis into the provisions of the IT Act and the rules notified therein along with the Intermediary Guidelines and Digital media Ethics Code (Rules 2021) makes it clear that it provides for a far better protection than before but, however, it needs to be considered how strictly and effectively it is implemented.

The motto of Digital India, "Power to empower," is genuinely achieving the desired results. In India, there are currently over 75 crore cellphones, 133 crore Aadhar cards, over 80 crore internet users with 4G, and the country is rapidly moving towards 5G.

India is now the fintech innovation ecosystem with the quickest rate of growth. Innovative digital payment solutions like Aadhaar-Enabled Payment Systems (AEPS) and UPI made this possible. Cash was delivered right to customers' doorsteps using AEPS-based micro-ATMs located at CSCs and post offices during the Covid-19 bank and ATM closures.

As of March 2022, India boasts over 61,400 startups, positioning it as the third largest startup ecosystem globally, following the US and China. With the rapid advancement of technology, digital platforms are also increasing be it about social media or entertainment platforms so rules and regulations are made from time to time and also amendments to IT law.

The paper has dealt with the concept of intermediaries, an assessment about how through rules notified, enactment and judicial pronouncement these network service providers are made liable, their scope, ambit &

the extent. The researcher attempts to analyze it through timeline of intermediary liability in India and the various rules notified under the IT Act from time to time, in order to deal with the challenges involved.
As the statutory regime governing intermediary liability for third party content in India is found primarily but not exclusively, in section 79 of the IT Act 2000, IT (Intermediaries Guidelines) Rules, 2011 as well as the copyright Act whereas separately S. 69A of the IT Act, and the Rules under Sec. 69A, provide for a procedure for the govt. to take down third party content, which makes the intermediary liable to a penalty.
Despite of the above provisions the liability of the intermediaries could not be determined which resulted the introduction of IT (Intermediary Guidelines & Digital Media Ethics) code, Rules, 2021. However, these rules have certain infirmities which have been discussed by the researcher from various perspectives. Moreover, subsequently in June, 2022, MeitY released the proposed draft amendments to the IT rules, 2021.
Thus, according to the study, laws governing intermediaries' activities are fundamentally required, but they shouldn't be overly onerous since this would hinder advancement and prevent intermediaries from developing new facilities.
Due to its strong emphasis on individual rights, the United States is frequently the first country to enact legislation safeguarding these rights. The DMCA is a relatively extensive set of regulations that control the liability of ISPs, especially because it was among the first laws addressing ISP liability. The DMCA operates under the premise that ISPs are immune from liability for copyright infringement by their customers as long as they have complied with the Act's requirements. The DMCA can be improved in a few ways, including by including measures to reduce needless litigation that harm ISPs' resources, productivity, and reputation. Strong action should be taken against those who file bogus copyright claims and pressure the ISPs to delete specific content from their websites, in addition to the legal fees and damages stipulated in Section 512(f).
In light of the situation, it is commendable that India has attempted to address the issue of restricting ISP liability through the IT Act, 2000. To guarantee a fair balance between IPR holders, ISPs, and other technological stakeholders in a nation that is developing quickly like India, it must be comprehensive.
Given that the Internet transcends national boundaries, some argue that it is preferable to have a set of internationally recognized guidelines governing ISP liability. If this kind of measure were to be adopted by the global community, it would be a better means of protecting the rights of those who own intellectual property rights, as well as those of ISPs and other relevant parties, and it would undoubtedly benefit the global economy in general.

Suggestions:

At National level

1. Looking at the rapid technological advancement, it can be said that merely providing appropriate legislative & regulatory mechanism is not enough rather effective remedies for redressal to the victims of various unauthorized unwanted criminal activities done in cyber space & social media, must be provided.
2. In order to bring OTT platforms & their content under the ambit of the relevant sections of the IT Act, these platforms should come under the purview & scope of the definition of intermediaries as provided under section 2(1)(w) of IT Act 2000.
3. A self-regulatory mechanism is unavoidable in this regard because technology is advancing at an accelerated rate and surpassing physical boundaries on a daily basis, making it impossible to manage digital media platforms only through legislation.
4. In addition to costing artists and content creators their livelihoods and the freedom of expression that is fundamental to democracies, censorship can also hinder innovation. Therefore, restricting all rights is not the best course of action, but Art. 19(2) permits the imposition of some limitations.
5. Legislations on sensitive issue must be passed through due process of law, after debate in parliament instead of relying upon executive rule making powers u/s 69A of IT Act.
6. There should be a balance between reasonable restriction and privacy which means reasonable restrictions and privacy should coexist in harmony since we need methods that increase security without sacrificing privacy.
7. In order to effectively oversee the content on over-the-top (OTT) platforms without violating individuals' rights, an impartial regulating authority is also required.
8. To avoid conflicts, laws should unambiguously define and classify content as either legal or illegal; rules should be precise and unambiguous in this regard. Furthermore, laws must pass the requirements of necessity and proportionality for the general public to understand them.
9. Intermediaries perform a wide range of tasks and are categorized under several headings, the most prominent being social media platforms, e-commerce platforms, and search engines. However, it is unclear from the IT Act's current statutory framework which intermediaries are subject to what obligations. Not even court rulings have offered conclusive answers in this area. Therefore, in order to properly define what constitutes "due diligence" from various kinds of intermediaries, it is necessary to reevaluate the statutory framework established under section 79 of the IT Act.
10. Looking at the dynamics of technological advancements it seems that India needs a more robust and comprehensive law extending the liability of ISP's covering, every major aspect in this context which is clear, transparent and promotes speedy execution, in terms of both, prevention of crime and execution of penalty.

In addition, intermediaries must support the investigations; otherwise, they risk facing legal repercussions such as fines, license revocation, or suspension from offering internet services if they fail to follow a set of guidelines for tracking, monitoring, and assisting law enforcement in combating cybercrimes.
11. The Indian population reported the highest amount of fake news among Internet users in 22 countries, according to recent studies (e.g., Microsoft News Center India, 2019). Messages on social media and messaging services are frequently circulated with false and inaccurate medical advice. The government has made several attempts to address this issue; the most recent being the tracing the first originator clause in IT Rules 2021. However, this will not be sufficient unless the term "Fake News" is defined separately.
12. Despite Technology changing at an exponential rate yet the concept of media remains the same. The term 'digital media' although defined under IT Rules 2021 nevertheless, there is vagueness in the definition, it still does not include the replica & e-newspapers, does not cover news operations under the press council Act 1978 and Cable Television Networks Regulation Act 1995, respectively. So, instead of embodying it in rules, the definition of digital media must comprehensively be incorporated in IT Law.
13. One thing that is crucial is that nothing can be accomplished unless it complies with the law, whether they be government authorities, private sector self-regulatory organizations, or intermediaries i.e., the rule of law must also apply on social media. The Shreya Singhal ruling abolished S. 66-A of the IT Act, although it is still in effect. The right to privacy was acknowledged as a basic right under Article 21, yet there are no established guidelines for digital platform governance.

At Global Level:

1. Regarding intermediary liability, democratic nations outside the United States typically employ one of three approaches: the awareness or "actual knowledge" approach (found in Australia, India, Japan, and the Philippines); the "notice & takedown" approach (found in New Zealand & South Africa); or the "mere conduit" approach (found in the EU, South Africa, and India); in contrast, "safe harbor" is found separately in sections 512 of the US Copyright Act and 230 (C) of the Communication Decency Act. Nevertheless, no set of rules or regulations is universally adhered to by all nations. The range of intermediates is expanding at this time. Thus, at the national level, nations must adopt or enact laws that incorporate some of the advantageous characteristics of other nations, while at the international level, a full code is necessary to guarantee forced conformity.
2. Social media intermediaries must incorporate the Santa Clara Principles on Transparency & Accountability in content moderation to their letter & spirit. As it will further enable well rounded regulations.
3. Manila Principles on Intermediary liability for limiting liabilities for content to promote freedom of expression innovation must be adhered to.
4. Globally, the "right to data privacy" needs to be acknowledged as a human right, and international bodies need to set rules for data security that might serve as the foundation for different national laws. For the reasons that only they can provide, governments everywhere must make room for a digital future; but this should not be done at the expense of peoples' fundamental human right to privacy.

After analyzing the whole scenario, the researcher is of the view that ISPs role and participation has been growing with passage of time and more and more advancement of technology. However, there are certain infirmities in the existing legal framework for the regulation of this developing role and functioning of the Internet Service Providers. Therefore, the above mentioned are the suggestions put forth by the researcher which are recommended to be incorporated at national and international level.

1. Collins English dictionary-complete and unabridged Harper Collins publisher http://www.free dictionary .com
2. Chander 2014 a law and geography of cyberspace.
3. Report released on India's trillion-dollar digital opportunity-MeitY, 2022
4. Report released by MeitY 2022, India's trillion-dollar digital opportunity
5. Iamai-Kantar I Cube 2020 Report.
6. Mr. Apurva Chandra, Secretary, Ministry of Information and Broadcasting (MIB)) Statement.
7. http://www.naavi.org/naavi_comments_ITAA/historic al perspective.
8. https://meity.gov.in>files
9. https://www.meity.gov.in/meity-business-rules
10. https://www.outlookindia.com/newsscroll/noproposal-regarding-legislation-for-regulation-of-ottservice- providers-at-present-dhotre/ 1937096
11. W.P. No. 32128 of 2019
12. M.A. No. 435 of 2021
13. The Cinematograph Act, Section 5D
14. The Cinematograph Act, Section 5A
15. www.govt.economictimes.indiatimes.com
16. Information Technology Act, 2000
17. EU Directive 2000/31
18. The Digital Millennium Copyright Act, 1998

19. Christian Louboutin SAS v/s Nakul Bajaj and Ors. (2014 SCC Online Del. 4932) Para 43.
20. SC 0329/2015
21. Itu.int/Global Cyber security Index/2020
22. Report of Ad hoc Committee of Rajya Sabha to Study the Alarming issue of Child pornography on social media & its effect on children and society at large.
23. Suo Motu W.P. (Criminal) No. 3 of 2015, Prajwala v/s Union of India & Others
24. Pib.gov.in
25. 31st Report of the committee on subordinate legislation of Lok Sabha on Rules under the it Act, 2000.
26. White Paper of the committee of experts on Data protection framework for India under the chairmanship of Justice B.N. Shrikrishna.
27. (2017) 10 SCC 1, 262
28. 116 (2005) DLY 427, available at https://indiankanoon.org/doc/309722
29. 2011, Delhi High Court (336)
30. (2016) Del. SCC 6382;(2017) 236 DLT 478 (DB)
31. 2019 SC Online SC 1587
32. (2014) SCC Online Del 4932
33. FAO (OS) 133/2019, Del HC, www.mondaq.com
34. MANU/SC/0329/2015
35. cit-india.org/copyright Act/rules/Intermediary liability Regime
36. www.mondaq.com/inida/social-media/intermediary rules and digital news/
37. Ministry of Electronics and IT Proposed Draft Amendments to the IT Rules, 2021, June 06, 2022.
38. Chicago Lawyers' Committee for Civil Rights Under The Law Ine v Craigslist Inc, Case No. 06 C 0657 (N D III, 14 November 2006) in Online Defamation/Libel/ Communications Decency Act-Internet library of law and court decisions. http://www.internetlibrary.com/topics/ online defamation.cfm (24 May 2007