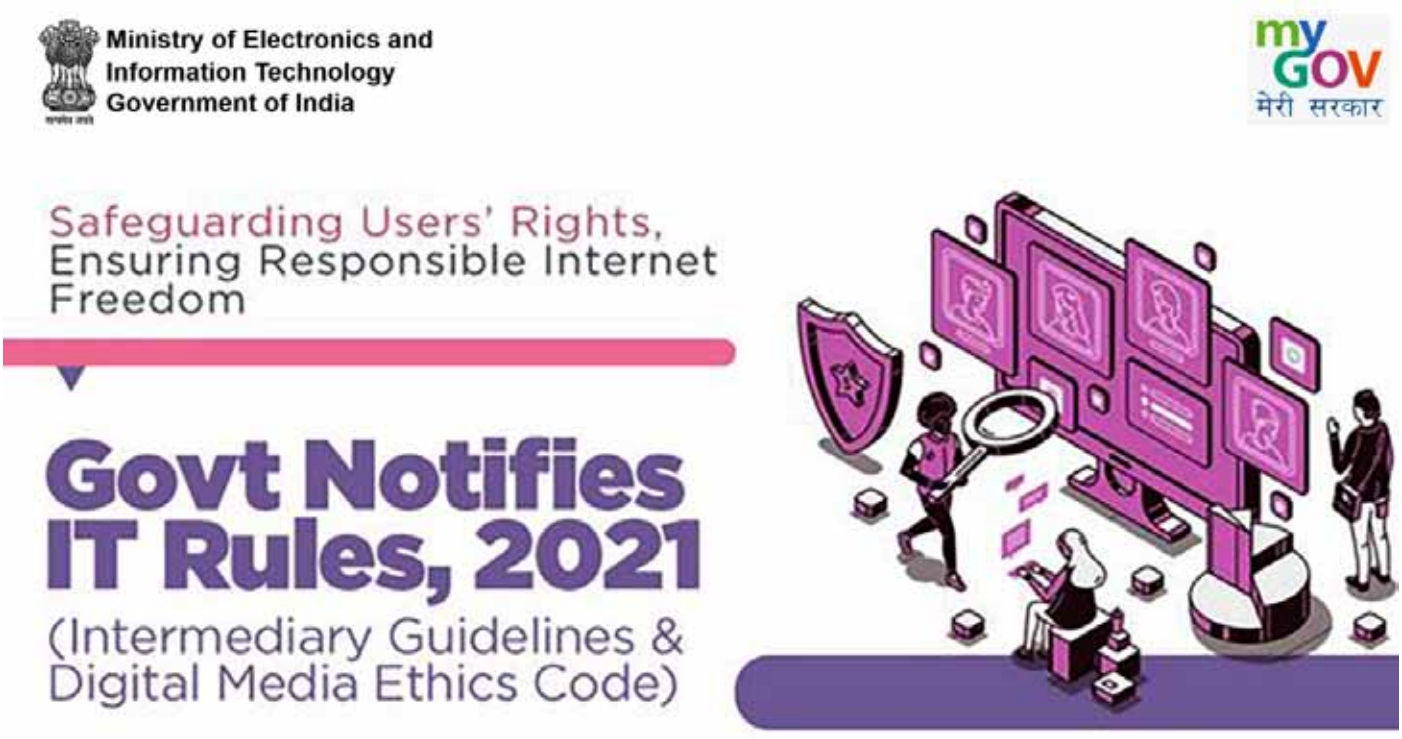
SHARPENING LIABILITIES AND OBLIGATIONS CAST UPON INTERMEDIARIES: AN ANALYSIS IN THE BACKDROP OF THE 2021 RULES

Intermediary: The concept

Intermediaries are gateways to the internet- services enabling delivery of online content to the end user. The various players involved in the chain range from ISPs (Internet Service Providers like Airtel that help users to get connected to the net by means of wired/wireless connections), search engines (the most commonly used ones in India being Google Search, Yahoo Search, Microsoft Bing and Duck Duck Go), DNS providers (that translate domain names to addresses that can be understood by computers), web hosts, interactive websites (which include social media sites like Facebook and Twitter) and even cyber cafes. The ambit of the term is wide enough to include any website that facilitates and brings together two interest groups (such as retailers and consumers in an online shopping mall), carriers of information (a classic example being Gmail service) as well as payment gateways (PayPal and Pay Tm to name a few). To be specific, Section 2(1) (w) of the IT Act, 2000 defines intermediary as "any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to electronic record.....".

However as time progressed, this definition (that derived much of its legal language from the EU e-commerce Directive of 2000) was broadened both in scope and in ambit. From the days wherein intermediaries were treated as monolithic entities-- as simple conduits or dumb passive carriers who could not and did not play any active role in the content--- the country has moved on to the era of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 wherein even curated content platforms such as Netflix and Amazon Prime as well as digital news publications have been roped in. Content takedown provisions for online news websites and online news aggregators have become the order of the day. All online streaming



platforms including Over-the–Top(OTT) come under the ambit of regulated entities . Needless to say, such a legal step was called for in the light of the diversification of services offered by the intermediaries and the significant issues of scale wielded by a few select players. As things stand today, the Rules envisage three types of entities, whose levels of obligations vary based on the hierarchies of classification:-

a. Intermediaries within the traditional meaning of Section (2) (1) (w) of the IT Act.

b. Social Media Intermediaries (SMIs) (i.e) entities which enable online interaction between two or more users (with less than 50 lakh registered Indian users)

c. Significant Social Media Intermediaries (SSMIs) (i.e) entities with user-thresholds as notified by the Central Government-- with more than 50 lakh registered Indian users (Facebook, YouTube, Whats App, etc.)

The Indian Response: Section 79 and Safe-Harbour Protection

Before the IT (Amendment) Act 2008 was passed, Section 79 dealing with liability of intermediaries was ambiguously worded. However, following the amendment, an umbrella protection is provided to intermediaries (i.e.) they are provided conditional immunity under the due diligence doctrine irrespective of the nature of the content. Whether an intermediary could claim safe harbour, hinges largely on two factors:-

a. Actual knowledge about the unlawful act,

b. Compliance with due diligence obligations and observing all other guidelines prescribed by the Central Government in relation to its duties.

To be specific, the conditionalities subject to which an intermediary enjoys exemption from liability are as under:-

i. The exemption applies only if the function of the intermediary is limited to providing access to a communication system over which information is transmitted , temporarily stored or hosted.

ii. The exemption applies only if the intermediary does not initiate the transmission nor selects the receiver of the transmission nor selects or modifies the information contained in the transmission.

iii. The exemption applies only if the intermediary observes due diligence.

iv. The exemption is not available if the intermediary has conspired, abetted or induced the commission of an unlawful act.

The exemption is not available if the intermediary fails to expeditiously remove or disable access to material upon receiving actual knowledge that any information residing in or connected to a computer resource controlled by that intermediary, is being used to commit an unlawful act.

2021 Rules and Offending Content

The 2021 Rules issued under the IT Act 2000 are intended to curb harmful content on social media. Expanding the ambit of the definition of user (under Rule 2(1) (x)), defining the concept of grievance (under Rule 2(1) (j)) and stipulating that an intermediary shall by way of its rules and regulations, privacy policy or user agreement *inter alia* inform its users that they must not host, display, upload, modify, publish, transmit, store, update or share any information that is defamatory, invasive of another's privacy, libellous, racially or ethnically objectionable, etc. In a step up from the 2011 Rules, this prohibited information now includes content which is published for financial gain but is patently false or information which is aimed at gender based harassment.

Offending content must be taken down within 36 hours of a court order and government notification to do so and government requests for data disclosure need to be met within 72 hours for investigation, detection or prevention of cyber security offences. Intermediaries must disable within 24 hours of a user complaint any content that depicts non-consensual nudity and sexual acts including morphed images transmitted with malicious intent.

Another important change is the requirement to appoint a grievance officer (also prescribed under the 2011 Rules) and publish his name and contact details prominently on its website. Building on the 2011 Rules, the 2021 Rules make it obligatory upon the grievance officer to acknowledge any order, notice or direction issued by a court or a governmental agency or a complaint received from an individual user or victim. Further a complaint must be disposed of within 15 days from its receipt (as opposed to one month under the 2011 Rules).

Significant Social Media Intermediaries are required to create a more accountable take down system, special expedited take down procedures for revenge porn cases, appointment of India based compliance officers (Chief compliance Officer under Rule 4 (1) (a), nodal contact person under Rule 4(1) (b) and Resident Grievance Officer under Rule 4(1) (c), identification of a physical address for service of legal notices, etc. It is also stipulated that an Special Sensor Microwave Imager (SSMI) providing chiefly messaging services must enable the identification of the first originator of the information on its computer resource – a promising way to control malicious information. It must deploy technology based measures (including automated tools) to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct - whether explicit or implicit. It must also appoint a senior employee, who would be criminally liable for non-compliance. As per Rule 7, an intermediary would forfeit exemption from liability enjoyed by it under the law if it were to fail to observe its obligations for removal /access disablement of offending content despite a court order to that effect. This makes the intermediary liable for punishment under any law for the time being in force (including IPC). On May 26, 2021, the Government of India issued a circular enquiring about compliance with the rules by all SSMIs.

It is worth mentioning here that while the IT Act did not originally envisage regulation of digital media, the 2021 Rules impose various obligations on digital media entities which carry out systematic business activity of making content available within India. Even foreign news publishers with an online presence in India shall be regulated by the prescribed Code of Ethics.

Technical Challenges in Removing Offending Content

The complexity of this scenario is amply clear from the words of Justice Anup Jairam Bhambhani of the Delhi High Court while delivering a judgement on April 20, 2021 laying down the procedure for removal of offending content from net:

"The internet never sleeps and the internet never forgets. The true enormity of this fact has dawned over the course of hearings conducted in the present matter when it transpired that despite orders of this Court, even the respondents who were willing to comply with directions issued to remove offending content from the world-wide-web, expressed their inability to fully and effectively remove it in compliance with court directions, while errant parties merrily continued to re-post and read-direct such content from one website to another and from one online platform to another, thereby cocking-a-snook at directions issued against them in pending legal proceedings..... the Court according perceived that the issue of making effective and implementable orders in relation to a grievance arising from offending content placed on the world-wide-web needed to be examined closely and a solution to the problem needed to be crafted out so that legal proceedings of the nature faced by this Court did not become futile. The Court cannot permit itself to resign to the cat-and-mouse game of errant parties evading court orders by reposting offending content.....in an act of defiance and contumacy."

Needless to say, migration of content as well as technical feasibility of filtering of defamatory contents poses insurmountable challenges. A classic instance within the framework of which these questions can perhaps be discussed is the Blue Whale Challenge. The notorious game that targeted young children to commit suicide is reported to have originated from Russia and hit India in 2017. The Government of India banned the game from access within the country, but the question of technical feasibility to implement the ban loomed large. For an intermediary, the game was not found on an exclusive website or app that can be blocked, but used encrypted communication channels through social media or direct messaging service, rendering the social account inactive on pages where it sneaks in was easier said than done.

Through a technique called photo DNA profiling(that uses hash algorithm as it will have the same hash value if the content is same and thereafter can be blocked by contacting the concerned service provider) was suggested, it needed multi-stakeholder action. However, it needs to be mentioned here that such intermediaries on whose sites a third party posts a Blue Whale link would not be held liable unless there is actual knowledge and/or conspiracy/intention to commit the crime (provided it has followed due diligence norms). Similar were the technical challenges in blocking child pornographic websites despite it being an offence u/s 67 B of IT Act. A silver line in the horizon, however is the fact that de-indexing of offending content globally does not require the search engine to take any steps around the world, but only to take steps where its search engine is controlled. This has been reiterated by the Supreme Court of Canada.

Conclusion

With the enactment of the 2021 Rules, the Central Government has sharpened and expanded various aspects of the liabilities and obligations cast upon intermediaries to deal with unlawful content. The Rules are broader in scope than the 2018 draft Rules. Faced with the conflicting scenarios presented by social media – its immense popularity on the one hand and the growing concern that the content can be defamatory, deceptive, paedophilic, hateful, inflammatory or otherwise harmful on the other hand, the authorities have stepped in to make sure that the delicate balance does not go wrong by prescribing 16 due diligence steps to be followed by intermediaries.

Recognizing that it is imperative to take immediate action (as any delay could render the same as ineffective and futile), timelines for disablement of access to *prima facie* unlawful material have been effectively reduced from those specified in the 2011 Rules. Mention needs to be made here that the 2021 Rules specifically provide that offending content may be removed in the first instance, giving to any interested person as specified in Rule 4(8) the liberty to object to such removal and to request for reinstatement of the removed content. This has been provided in the Rules as it affords a more fair and just balance between the irreparable harm that

may be caused by retaining offending content on the world-wide-web and the right of another person to seek reinstatement of the content by challenging its removal.

Rule 4(4) requires intermediaries to display a notice to any user attempting to access information identical in content to those that have previously been removed that such information has been access-disabled. The second proviso to Rule 4(4) contemplates implementation by a SSMI of appropriate human oversight of measures deployed under this sub-rule and periodic review of automated tools so deployed.

However, we must also recognize that it is too onerous and impractical for intermediaries to keep a lookout for offending content, particularly when it can resurface in various disguises and corrupted *avatars* at the instance of mischief mongers on a continuous basis, given the stark reality that a search engine is unable to appreciate the offending nature of content appearing in a different context. Despite these technical difficulties in the backdrop of the internet, it needs to be emphasized that if offending content cannot be completely removed, it can be made unavailable and inaccessible by de-indexing and de-referencing it from the search results of the most widely used search engines. Needless to say, for an order directing removal or access disablement of offending content to be effective, a search engine must block results throughout the world. The need of the hour is to harness technological tools to ensure that anonymity, seclusion of one's own space and privacy which are the hallmarks of cyberspace are not misused – making use of the anarchical nature of the net- to settle scores, at the same time ensuring that freedom of speech is by no means compromised or undermined. The choice before the nation, its lawmakers and citizens is clear. ■

AUTHOR

Dr. Raju Narayana Swamy

**(The author is an IAS officer of Kerala Cadre of the 1991 Batch.
At present he is the Principal Secretary to Government of Kerala)**