Volume 10, May 2020 ISSN 2581-5504

"Liability of Online Marketplaces and Social Networking Websites"

Raghav Agrawal
Jindal Global Law School

Abstract

The following paper attempts to provide an overview of the intermediary regulations in the sphere of online marketplaces in India, analyzing the judicial pronouncements and legislative enactments concerning the same. The paper shall endeavor to highlight some of the discrepancies in the current law and further evaluate whether the proposed 2018 Draft Guidelines are adequate in dealing with the same. The primary regulatory dilemma in such a scenario is to ensure that the growth of intermediaries is not hampered and that India continues to attract investment due to its ease of doing business while ensuring that these intermediaries are observing a minimum level of due diligence in the interest of public order and safety. Hence, keeping this objective in mind, the paper will attempt to analyze the adequacy of the current legal framework governing the liability of online intermediaries.

I. Introduction

The population of India is around 1.3 billion people, and there are about 241 million Facebook users in the country. Flipkart has over 160 million registered users, and they have roughly 32 percent of the market share. Amazon also has over 100 million registered users. These are examples of some of the most popular internet platforms that are accessed by millions of people every day. In a world where innovation cycles are progressing at such a fast pace, the need for the law to adapt to such changes and evolve becomes all the more significant. It is imperative that the perfect balance of continued innovation and regulation of misconduct is achieved through law. Legally, these online platforms come under the definition of intermediaries. An intermediary under the Information Technology Act, 2000 (hereinafter referred to as "IT Act") is defined as "*service concerning that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places, and cyber cafes*."[1] On a fundamental level, these websites perform the primary task of receiving, storing, and displaying information from third party users. Amazon and Flipkart are merely providing a platform that receives data from merchants and vendors across the country, which then stores and displays it to all possible customers. Facebook and other such social networking websites (Instagram, Twitter) are also just creating a format in which a user can share any information. The information is then shared in that specific format with all other users and stored.

Legally, online marketplaces and social networking websites can fall under the definition of intermediaries provided they follow specific rules. The act of merely providing the underlying infrastructure does not automatically expose these intermediaries to liability if

[1] The Information Technology Act, 2000 (No. 21 of 2000) available at : "https://meity.gov.in/writereaddata/files/itbill2000.pdf"

Volume 10, May 2020 ISSN 2581-5504

third party users use their platform for illegal or disparaging activities, but a close analysis of the law shows that if an intermediary is negligent and fails to fulfill its several obligations, they will be held liable. This conditional presumption of innocence is enshrined in the safe harbor provision in Section 79 of the Act and provides protection to intermediaries from any third-party act. Arising from the above-mentioned section are the *Information Technology (Intermediaries Guidelines) Rules, 2011*[2]. The Safe Harbour rules have evolved considerably since their enactment, partly through amendments of the underlying Act and rules, and partly through how the court interprets these provisions.

Through this paper, I attempt to first delineate the evolution of laws governing these online intermediaries in a world with constantly evolving technological developments. The next section deals with the Intermediary Guidelines of 2011, focusing on the scope of its provisions that are explained through case-laws. The fourth section deals with the Proposed Amendment to the Guidelines and highlights the benefits and drawbacks of implementing the same. In the fifth section, I attempt to make a comparative analysis of the Guidelines with the laws governing online intermediaries in the United States of America. And lastly, I end the paper with a brief discussion on the evolving nature of the market for intermediaries and the need for an effective regulatory framework for the same.

II. Evolution of the Current Law - Information Technology Act, 2000

The current jurisprudence and legislative developments regarding intermediaries can be segmented into pre and post amendments. The Information Technology (Amendment) Act, 2008 made several changes to the definition and broadened the scope of protection offered to intermediaries.

A. Pre-2008 Amendment

The first question that always arises in cases regarding intermediaries is whether it qualifies as an intermediary under the strict definition provided in the Act. With the emergence of new websites and applications every day that offer a varied array of services to customers, it is often tough to pinpoint whether they can be categorized as intermediaries or not. Initially, the definition of intermediaries was minimal.

Before 2008 the definition for an intermediary was very restricted.[3] It laid down a very narrow scope of what an intermediary entails, although the same is understandable considering that the IT Act was also passed in the year 2000, when such online platforms were just entering the Indian market. The protection offered to intermediaries at this point was only from liability of offenses under the IT Act. This namesake protection allowed them

[2] Information Technology (Intermediary Guidelines) Rules, 2011 available at: " https://meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf"

[3] Section 2(w) IT Act read: "(w) "*intermediary", with respect to any particular electronic message, means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;"*

Volume 10, May 2020 ISSN 2581-5504

to be exposed to all other legislations such as the Indian Penal Code, thereby making them vulnerable to prosecution.

The shortcomings of the definition were further highlighted in the 2004 case of *Avnish Bajaj v. State,*[4] wherein the managing director and the manager of the auction website was charged under sections of the Indian Penal Code and IT Act[5] for a CD containing obscene images that were being auctioned and sold on his website "www.bazee.com." They were also arrested for the same even though they were merely in charge of the website, i.e., providing the interface which acted as an underlying infrastructure for the third party to sell their products. The CEO was not involved in deciding which products are to be sold or the content of the products sold since this fell outside the purview of the website. The item was listed on the website for two days and was taken down as soon as a complaint was launched. The Delhi High Court found that a prima facie against them was sustainable, and they were charged under provisions of both the Indian Penal Code and the IT Act. The High Court also made a crucial point regarding the liability of such online platforms wherein it held that these intermediaries' liability needs to be graded on a scale, i.e., the amount of control that they can regulate and control on their platform would determine their liability. This would also be the basis of the intermediary regulation that was enacted in 2008.[6]

Holding intermediaries liable is not a new concept and is a derivation of *gatekeeper's liability*[7]. The concept has been followed while drafting several regulations wherein not only the offender is held liable but also the middle man. This can be seen in the example of underage drinking, where both the minor and the merchant who sold them the alcohol are held liable. This is a natural mechanism to ensure that unlawful conduct is contained, and a similar logic has been applied to intermediaries. Regulating conduct such as that in the *Avnish Bajaj* case (sharing of obscene content) is extremely difficult for law enforcement agencies due to the globalized nature of the internet where offenders can be in any jurisdiction and hide under the garb of anonymity. In such situations, it is more comfortable to hold the intermediary, i.e., gatekeeper, liable for undesirable conduct. This kind of reasoning and lack of safeguards for intermediaries did not draw much attention due to the nascent stage of the industry at that time, but the same did hamper the ease of doing business in India and restricted the flow of foreign investment and the creation of new business models.

[4] *Avnish Bajaj v. State*, Para 6, MANU/DE/1357/2004 (Delhi High Court).
[5] He was charged under the obscenity clauses under the IPC along with sections of the IT Act.
[6] The Avnish Bajaj case was later resolved by the Supreme Court in 2019 wherein the court dismissed the charges against the appeal on procedural ground. The Court stated that since bazee.com had not been mentioned as an accused in the suit, no action can be undertaken against the CEO of bazee.com.
[7] Chinmayi Arun, "*Gatekeeper Liability and Article 19(1)(A) of the Constitution of India*", NUJS Law Review (2014) available at: "http://docs.manupatra.in/newsline/articles/Upload/DA5C9359-8130-4A85-BFC1-53DED36DD551.pdf'

Volume 10, May 2020 ISSN 2581-5504

B. Post- 2008 Amendment

The *Avnish Bajaj* scandal, along with the rapid development of the information technology industry, did trigger a knee jerk reaction prompting the legislators to take action. The Information Technology (Amendment) Bill 2008 (hereinafter "2008 Amendment") lays down the framework for the current intermediary liability regime. The 2008 amendment aimed to align safe harbor provisions in the form contained in the European Union Directive on E-Commerce. Alignment with international standards is exceptionally essential for markets such as an online intermediary due to their globalized presence.[8]

Several changes were brought in by Amendment. Firstly, the definition of an intermediary under Section 2(w) was expanded. The safe harbor provisions under Section 79 of the IT Act now protected intermediaries from liability "under any law for the time being in force." This included the exclusion of the Indian Penal Code and, consequently, an automatic exclusion from the strict liability regime.[9]

The 2008 Amendment also shifts the burden of proof from the intermediary. Earlier, it was upon the intermediary to demonstrate that they were not aware of the illegal activity that took place on their platform for them to be absolved of any liability. This shifted after Amendment, and the default presumption is that they were unaware. These advantages under the safe harbor provisions are granted to all intermediaries provided they follow the basic guidelines mentioned under Section 79(2). The same requires the intermediary to not "initiate the transmission, select the receiver of the transmission, and select or modify the information contained in the transmission."[10]

III. Intermediary Guidelines, 2011

Section 79(2)(c) of the Act states that "*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*" following which the ***Information Technology (Intermediaries Guidelines) Rules, 2011*** were passed. It not only clarified the implications of words such as "due diligence" in Section 79 of the A but also laid down a structured regulatory framework for these intermediaries to operate within. The Guidelines specify due diligence requirements that need to be met by intermediaries to ensure that they are granted protection under the safe harbor provision. These include what regulations and rules the intermediaries should impose on their users, including the provision of a list of content which users are prohibited from sharing. The list includes content that harms minors in any way, infringes upon propriety rights such patents and trademarks, blasphemous content, and other such offensive content. The Guidelines also specified the process that needs to be followed in a situation where the intermediary has been informed of, or the intermediary has found out on its own that some information on its platform violates the standards laid down.

[8] Pritika Rai Advani, *Intermediary Liability in India*, 48(50) EPW 120 (2013).
[9] n 7.
[10] n 1, section 79.

Volume 10, May 2020 ISSN 2581-5504

Intermediaries are required to *remove* this content within 36 hours of *actual knowledge* of any such content being displayed on their platform. The implication of this 36-hour time period mentioned in the Guidelines was elucidated in the Clarification issued by the *Ministry of Communications and Information Technology* in 2013.[11] It clarified that the intermediary is required to "*respond or acknowledge*" the complaint within the 36-hour period, not necessarily take it down. This ensures that an unusually high burden is not imposed upon the intermediary, and due process of law is followed before any allegedly infringing content is taken down. The Guidelines have also led to discussions regarding what constitutes *actual knowledge* and what are the implications of taking the content down, discussed in the following section in further detail.

A. What constitutes "*actual knowledge*"?

Before the *Shreyas Singhal vs. Union of India*[12] case, the position regarding the action that needed to be adopted by the intermediary in situations where infringing content was on their website with their "actual knowledge" was unclear. The first question that naturally arose from this was the way *actual knowledge* should be construed. The Guidelines stated that this requirement would be fulfilled "*upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information*." Before the above-mentioned judgment, the interpretation of this section varies. It placed the intermediaries in a conundrum because they would receive several complaints regarding the content on their website and were unsure about how to act. If they were to accept all and remove all allegedly infringing content blindly, then it would put a barrier to freedom of free speech and expression. If they evaluated all complaints and if their evaluation did not align with the evaluation of the same if done later by a court, then they would be open to liability. Finally, this directly impacted the business interests of the intermediary since their intent is to provide the platform merely and not be regulators of content.

The *Shreya Singhal* case is a landmark judgment which not only upheld the right of free speech and expression but also read Section 79 of the IT Act along the with relevant Guidelines. The law laid down in the case was "*actual knowledge(implied) from a court order or on being notified by the appropriate government or its agency*." This approach, adopted by the Supreme Court in the judgment, had equal benefits and drawbacks. The benefit was that the burden shifted from the intermediaries to the courts to decide what content was unlawful and gave them a little more space to operate within. The obvious drawback of this mechanism is that now affected parties would need to adopt the long and arduous route of court orders to ensure any disparaging content about them on the internet is taken down.

[11] "Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011 under section 79 of the Information Technology Act, 2000" (18/03/2013) available at: "https://meity.gov.in/writereaddata/files/Clarification%2079rules%281%29.pdf"

[12] *Shreya Singhal v. Union of India*, Para 119, MANU/SC/0329/2015 (Supreme Court of India).

Volume 10, May 2020 ISSN 2581-5504

This is a clear departure from the concept of gatekeeper liability because responsibility is now imposed upon intermediaries to act as and when they are made aware of such conduct through the mechanisms specified by law. In the Indian scenario, it is a court order. Only if an intermediary fails to fulfil its responsibility to act when in possession of *actual knowledge* will there be a liability imposed upon it.

In the famous case against MySpace Inc.[13], Super Cassettes Industries Ltd. sued the platform MySpace for alleged copyright infringement of its content on the platform. In an interim order passed by the Delhi High Court, it held MySpace liable for the infringement, disregarding its claims of Super Cassettes refusing to submit songs to its song ID database, its lack of knowledge of such infringement, and its immediate removal of the infringing content upon receiving complaints. Directing MySpace to pre-screen all user-uploaded content, it upheld the complaint filed by Super Cassettes. However, the interim order was overruled by a division bench of the Delhi High Court on the grounds of a lack of "actual knowledge" of such infringement on the part of MySpace. It held that MySpace merely had a general awareness of such infringement. Furthermore, it was held that under the extant copyright laws, specific knowledge of the infringement from the content owner in the format provided by the platform is more than sufficient to impose liability, negating the need for a court order to this effect. Therefore, the MySpace judgment carved out an exception to the Supreme Court's ruling in the *Shreya Singhal* case wherein it held that specific actual knowledge of the infringement could only be imputed upon a platform once a court order informing the platform of the infringing content is enforced.

The *MySpace* case is crucial because it also provides relief in specific cases from the difficulties in obtaining court orders. It will be interesting to see how future judicial decisions aim to carve such exceptions in different fields owing to the varied services provided by intermediaries.

B. What constitutes a "takedown"?

All intermediaries operating in India are required to take down any content which is offensive under Section 79 of the IT Act. This raises an obvious question – what constitutes a takedown? In the recent judgment of *Swami Ramdev & Anr. V. Facebook, Inc & Ors*,[14] the Delhi High Court, expanded the ambit of this requirement, necessitating takedown of *any* content deemed unlawful under Indian laws from the entire computer network of the concerned intermediary. The case originated from a defamation suit filed by Baba Ramdev against a book titled "*Godman to Tycoon - the untold story of Baba Ramdev*" wherein the book was only allowed to be circulated after individual offending sections from the same were deleted. Videos containing the deleted sections were released on platforms of Facebook and other respondents in the case. Baba Ramdev approached the High Court seeking an order

[13] *Myspace Inc. v. Super Cassettes Industries Ltd.* MANU/DE/3411/2016 (Delhi High Court)
[14] *Swami Ramdev and Anr. vs. Facebook Inc. & Ors*, CS(OS) 27 of 2019.

Volume 10, May 2020 ISSN 2581-5504

to take the videos down. The court unequivocally held that if the content has been uploaded from India, then a takedown of the same can be directed, and if the content has been uploaded outside India, then they can prevent it from being accessed in India.

This requirement of a takedown provides an extraterritorial aspect to the applicability of Indian laws by necessitating takedown of offensive content from a platform, wherever it may be located across the world**.** The judgment is highly questionable since it imposes an unusually high requirement upon these intermediaries to track the source/ user that posted the infringing content and act based on their location. This implies that there is a need the intermediaries to track their users, raising serious concerns about the data privacy of users who access the platforms of these intermediaries. There has been no further clarification in this regard, but the respondents in the case have appealed to the Supreme Court, wherein it has been listed for arguments.

IV. Proposed Amendments to the Intermediary Guidelines, 2011

In 2018, the proposed amendments to the 2011 Guidelines were circulated by the Government for comments and feedback. The Draft Information Technology (Intermediaries Guidelines (Amendment) Rules) 2018 are yet to be notified by the Central Government. These are the proposed amendments to the existing law and might be able to tackle only some of the issues. The research will also be highlighting some of these shortcomings.

These draft guidelines have been widely criticized and opposed by many stakeholders in the technology sector. The Guidelines significantly changed many of the obligations imposed upon intermediaries, requiring them to now enact stricter due diligence practices, mandatory assistance to state agencies, a more proactive takedown requirement, and monitoring of content.

The current Guidelines require that the terms of use of intermediaries must include all the relevant information regarding what constitutes prohibited content. The list containing all the said prohibited content is currently provided in the Guidelines, and the same has been expanded by the Ministry to include all content that promotes consumption of tobacco and intoxicating products. There is also an additional requirement upon intermediaries to ensure that these terms and conditions of use are prompted to users every month to ensure compliance.

The proposed guidelines also required the intermediaries to be incorporated and registered in India with a physical address and office. This requirement is only for intermediaries who have over 50 lakh users. The physical office in India can also have adverse income tax implications for intermediaries who will then have a "fixed place of business" in India. This significantly raises costs for large intermediaries to operate in India and hampers the flow of new investment. This also disincentivizes foreign intermediaries from entering the Indian market since it ensures that once a certain threshold of users has been reached, there is a need

Volume 10, May 2020 ISSN 2581-5504

for a physical office. Consequently, overhead costs and taxes also significantly change, thereby creating new hurdles in the "ease of doing business" in India.

A. Mandatory Assistance to State

This is one of the most debated additions to the guidelines. This new obligation imposed upon the intermediary requires it to provide any assistance to law enforcement agencies within 72 hours of their request. The intermediary is also mandated to *"enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorized."* The purpose of the request can be related to the "*investigation, detection, prosecution, or prevention of offense.*"

The above-mentioned section grants law enforcement agencies unfettered power with regard to the commission of offenses on the internet. Further, the section's broad wording enables law enforcement agencies to bring any offense within its ambit. The requirement to enable tracking of users creates not only logistical and economic issues for these intermediaries, but also raises a larger question about the right to privacy and extent of government intervention. Firstly, it assumes that all intermediaries have the requisite competence and capacity to carry out such functions. It treats these intermediaries as well-established platforms with exceptional financial strength and public reach. However, many start-ups and new businesses aiming to develop and maintain intermediary platforms will find this requirement extremely tough to satisfy. Their financial incapability will exclude them from the protection under the safe harbour provision. The draft guidelines do not specify what kind of assistance will be required by law enforcement agencies, to what extent will such assistance be needed, and whether failure to meet these not yet specified standards will lead to exclusion from the safe harbour provision. Secondly, enabling a tracking requirement through intermediaries creates issues regarding what kind of information will be sought, who will be allowed to access it, and what purposes it can be used for. Though the guidelines do answer some of these questions, the answers provided are broad and ambiguous, indicating that such a tool is prone to misused very quickly. The chances of misuse are also extremely high in a situation such as a takedown Requirement, and monitoring of content, takedown requirement has been further expanded and clarified in the guidelines. Keeping in line with the *Shreya Singhal* judgment, intermediaries are not required to take down all content upon receiving an order from a court within 24 hours. The intermediary is also required to preserve a record of the same for up to 180 days.

The intermediary is now also required to have "*automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content*." This is a new inclusion in the draft guidelines, which further expands the list of obligations imposed upon intermediaries. The modalities of the same have not been expanded upon; neither are the standards which these "*tools*" would need to meet laid down. This ambiguous wording leaves the door open for intermediaries to lose their safe harbour protection and also requires these platforms to have such *tools* as part

of their system from the very beginning. This will discourage not only new companies but also global intermediaries from entering the Indian market where necessary protection under the law is provided at such a high cost. It also shifts the position of the intermediary as a passive platform of information to a more active participant in collecting information. Based on the reasoning in the *Avnish Bajaj* case, the more control the intermediary has on the content, more will the increase in its liability be; it is a proportionate increase that in my opinion is a justified stance.

V. Comparative Analysis using the Intermediary Laws in the USA

The US has seen the emergence of several global internet platforms that act as intermediaries by providing content for users. Naturally, it witnessed a lot of third-party claims against such intermediaries demanding accountability for the conduct of their users. This led to apparent demands by intermediaries for immunity from such third-party claims, which severely affect their financial position and reputation. Similarly, the content owners worry about the infringement of their intellectual property by third parties and consequently place premiums on their content usage. In balancing the business interests of both stakeholders in an emerging global market fuelled by increasing access to the internet, the US government struggled to recognize its role in this scenario. It ultimately prioritized the interests of the intermediaries over the content owners, providing extensive immunity to the intermediaries under the US laws.

The law regarding third-party liability for intermediaries is enshrined in Section 230 of the Communications Decency Act, which absolves any "interactive computer service" provider or user from any third-party liability. It also provides for a "Good Samaritan" immunity, which absolves the providers and users from any liability, should they take action to block offensive content on their platforms. By refusing to treat the intermediaries as the publisher or speaker of the content on their platforms, the laws seek to broaden their immunity and protect their business interests. The other legislation supporting the interests of intermediaries is the Digital Millennium Copyright Act ("DMCA"), which adopts the safe harbor approach. Similar to the approach prevalent in India, Section 512 of the DMCA provides a conditional safe harbor for intermediaries against claims of copyright infringement. It also has a "notice takedown" policy that allows owners of copyrighted content to "notice" and inform the intermediary of any infringement and "take it down" from their platform. [15]

In the case of *Doe v. Myspace*,[16] a claim of negligence was brought against Myspace for failure in implementing safety measures to prevent minors from lying about their age and accessing their platform. These minors then access the platform to meet new people and thereby communicate with potential sexual predators. Recognizing the absurdity of such a

[15] NDA, "*India: Intermediaries - Messengers or Guardians?*" 28 Feb 2019, available at: 'https://www.mondaq.com/india/copyright/784524/intermediaries-messengers-or-guardians-how-india-and-us-deal-with-the-role-and-liability-of-intermediaries'
[16] *Doe v. MySpace, Inc.*, 528 F. 3d 413 (5th Cir. 2008)

Volume 10, May 2020 ISSN 2581-5504

claim, the US courts held that Myspace was not liable for any wrongdoing. It exercised due caution while allowing access to users and cannot be held liable for any communications by third party users. Its task is merely to provide the platform upon which users can meet and connect, anything more would amount to a breach of privacy of its users. Similarly, in *Viacom Int' l Inc. v. YouTube Inc*.,[17] the courts upheld the broad immunity provided to intermediaries by imposing the burden on the content owners to show specific knowledge of instances of infringement by the intermediaries. This depicts the clear priority given to intermediaries' interests since the only other manner in which they could be held liable was if content owners could prove that the intermediaries exercised "substantial influence" over the infringing activity of the users. Only upon content owner's discharge of the burden of specific evidence indicating knowledge or substantial influence can the intermediaries be held liable for the third-party infringements. Thus, there is a much broader immunity offered to intermediaries in the US in comparison to India, with the US government prioritizing the business needs of this emerging market to capitalize on its gains for the economy.

VI. CONCLUSION

The paper attempts to illustrate how opting entirely for any one side i.e. zero supervision over the functioning of intermediaries, or complete control and supervision over their functioning, creates a multitude of issues. The trajectory of the legislature in enacting rules and guidelines in this market clearly depicts their struggle in finding a middle ground that balances interests of all stakeholders; however, there is evidently still a long way to go. The draft guidelines do a commendable job in codifying various aspects that required clarity in the Guidelines, but rules like those mandating tracking of users also raise serious concerns of government censorship and the right to privacy.

Information that is not permitted in the public sphere usually finds its way online. This is not only applicable to explicit prohibitions of specific information but also subtle prohibitions. This can be most clearly seen in the recent explosions of online magazines such as The Wire. Consumption of current affairs through the online mediums has not only led to a decay in the print media industry but also allowed for articles and editorials that were not printed in newspapers to be available online. Easy access to information has created a vibrant culture of dissent and healthy discourse regarding pressing issues, without the problem of government censorship. Creating mechanisms that now allow private, for-profit bodies like these intermediaries to govern and track users and information acts as a means of thwarting such free flow of information and criticism that is imperative to sustain a healthy democracy.

This paper merely attempts to demonstrate the two opposing interests of the regulators and online intermediaries, highlighting the need for a closer look at the laws governing the latter. The ongoing pandemic makes it even more imperative to have debates and stimulating discourse on intermediaries and the laws governing them. COVID-19 has raised the importance of intermediaries, since staying at home has increased the frequency in usage of

[17] n 15: .07 Civ. 2103 (S.D.N.Y. April 18, 2013).

Volume 10, May 2020 ISSN 2581-5504

digital economies, online media, and other such platforms while conducting the day-to-day affairs. By no means is the work of the legislature over in this field and the pressing issues generated by the proposed amendments in this paper necessitate government intervention at the earliest.