JOURNAL OF CYBER COVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 12

Safe Harbour Protections and their Misuse by Digital Platforms to Evade Liability

Ayushi Singh

National Law University Odisha

Recommended Citation:

Singh (2026) "Safe Harbour Protections and their Misuse by Digital Platforms to Evade Liability" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 12. (DOI)

ABSTRACT

The growth of online platforms has led to various problems related to the free flow of information and legal limits. To create a balance between the two, safe harbour provisions were designed, this functions as a cornerstone of modern internet regulation. The objective of safe harbour protection was to protect intermediaries from liability based on third party content, but significant challenges regarding the application of these laws, especially relating to their possible misuse in order to escape accountability are exposed.

Through this paper, the legal framework of safe harbour protections in India is critically examined and compared to global developments. The statutory provisions under the Information Technology Act, 2000, guidelines such as the Intermediary Rules, 2021 and judicial interpretations are analysed. This research recognizes the way through which platforms try to exploit the law in order to avoid accountability.

Through comparative and doctrinal analysis, the tension that exists between free speech and accountability, gaps in enforcement and lack of due diligence are highlighted. Based on this research, it has been concluded that safe harbour protections are essential, but regulatory objectives are undermined as a result of their misuse. This paper recommends strong enforcement mechanisms along with clearer standards and balanced methods to ensure innovation and accountability together.

KEYWORDS

Safe Harbour, Digital Governance, IT Act 2000, Platform Accountability, Intermediary liability, Social Media Regulation

INTRODUCTION

In recent times, content hosting services such as social media platforms and search engines have become central to public discourse, through means such as commerce and governance. The fundamental method of creation, consumption and sharing of information has been transformed as a result of the rise of digital platforms. However, this also raises intricate questions and creates confusion about the legal liability of platforms hosting user-generated content.

In order to reduce the confusion, conditional immunity from liability was granted to intermediaries through Safe Harbour provisions. Section 79 of the Information Technology Act, 2000[1] contains this protection in a codified way, intermediaries are protected from liability arising from third party content, provided that they maintain compliance with certain due diligence requirements. In the same way, Section 230 of the Communications Decency Act in the United States provides similar provisions[2].

Although the original intent behind safe harbour provisions was to promote free expression and innovation, there has been increased scrutiny against it. It has been argued by critics that these protections are exploited by digital platforms in order to escape responsibility for harmful content such as hate speech and misinformation[3]. This has resulted in increased apprehension about the effectiveness of these regulatory frameworks and the accountability of intermediaries.

The research question of this paper is to find out to what extent digital platforms evade liability by using safe harbour provisions and how this misuse is addressed by legal frameworks.

The core objectives of this research are to first analyse the legal frameworks governing safe harbour protections, then examine judicial interpretations and identify patterns of misuse and finally propose solutions and reforms.

A comparative and doctrinal approach has been adopted by this paper to examine case laws and statutory provisions.

[1] Information Technology Act 2000, § 79.
[2] Communications Decency Act, 47 U.S.C. § 230.
[3] Eric Goldman, ‘Why Section 230 is Better Than the First Amendment’ (2019) 95 Notre Dame L Rev 33

LITERATURE REVIEW

Legal scholarship has widely debated the concept of safe harbour, specially in the context of intermediary liability. It has been emphasised by early literature that these protections provided to intermediaries are necessary to ensure free speech and foster innovation[4]. It has also been emphasised by early scholarship that intermediaries are mere conduits for information and thus should not be held liable for content created by users. Imposition of strict liability on such platforms could possibly stifle the growth of the internet and also discourage user participation, and it will also be unfair for those platforms which are just functioning as a means of flow of information. Stringent control could backfire as the effective functioning of these intermediaries or third-party hosts are essential for the flow of information in the digital age.

If we talk about the United States, there is a description of "the twenty-six words that created the internet"[5] This description is attached to Section 230 of the Communications Decency Act. Section 230 functions as the cornerstone of internet regulation. To prevent platforms from being treated as the publishers of third-party content, broad immunity is provided to them, but this immunity is criticised for enabling platforms to evade responsibility when they host harmful content. The expansive scope of this immunity is subjected to increasing criticism and questions regarding the evasion of accountability by platforms through this protection.

Now, comparing this to the Indian framework, Section 79 of the Information Technology Act, 2000[6] lays out provisions to provide conditional immunity to intermediaries. In the case of *Shreya Singhal v. Union of India*[7]*The* Supreme Court of India has clarified that intermediaries need to remove content only after a court order or government notifications asks them to do so. This judgement is considered a momentous step in maintaining accountability of intermediaries while also protecting freedom of expression. This approach has tried to create a balanced solution in order to accommodate freedom of expression as well as accountability and responsibility.

[4] Jack Balkin, Free Speech in the Algorithmic Society, 51 U.C. Davis L. Rev. 1149 (2018).
[5] *Jeff Kosseff, The Twenty-Six Words That Created the Internet (Cornell Univ. Press 2019).*
[6] *Information Technology Act, 2000.*
[7] *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*

Further developments, including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[8]These rules introduced more stringent due diligence requirements, transparency mechanisms and grievance redressal mechanisms. It has been noted that these rules tried to create a balance between user rights and platform accountability, but concerns about threat to privacy and overregulation still prevail.

Another significant domain of discussion concerns the tension between accountability and immunity. The broad application of Safe Harbour provisions can lead to misuse by the intermediaries. It is possible that platforms deliberately won't moderate harmful content so that they can retain user management, which would lead to exploitation of legal protections.

Enforcement is another important area of debate; it has been shown by studies that regulatory authorities often don't have the requisite capacity to efficiently monitor and enforce compliance. This leads to the creation of a gap between practical outcomes and legal provisions[9].

There exists a lack of comprehensive analysis of how safe harbour provisions are used strategically by platforms to escape liability. This gap is addressed by this paper through the examination of real word practices along with legal practices.

METHODOLOGY

This research is done using doctrinal methodology by focusing on analysis of judicial decisions, regulatory frameworks regarding safe harbour protections and statutory provisions. Primary sources used for the research include the Information Technology Act, 2000, relevant rules and landmark judgements.

Analytical approach is also employed to examine the practical outcomes of safe harbour provisions and analysing the patterns of misuse by digital platforms, case studies and examples are also used.

The study further incorporates a comparative approach to compare and analyse the legal frameworks in other countries, particularly, the United States and the European Union. Assessment of effectiveness and identification of best practices can be done through comparative analysis.

[8] *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.*
[9] OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives (2011).

This methodology is chosen as it helps focus on policy analysis and legal interpretation, thus serving as the appropriate methodology.

ANALYSIS

The Safe Harbour Provisions were conceptualised in the first place to confront the unique challenges posed by the internet. Intermediaries act as facilitators of communication, they are not the creators of information[10], this is a necessary difference between them which was recognised before laying out provisions and rules regarding intermediary liability. Example – Instagram is a platform for sharing content, anyone can share whatever content they want to, Instagram merely functions as a platform. Now if some legally objectionable content is shared, then should responsibility be inflicted on the third-party app, which is Instagram in this example. It is in this context that we understand the objective difference between host and publisher of content, the host should be provided certain protections when some harmful content is published through them. Thus, Conditional immunity is provided to ensure that content created by users does not become the reason for imposition of liability on this party platforms which are merely host of the content, not publisher[11]. It is important to ensure that intermediaries are not treated as publishers, subject to the condition that they comply with necessary conditions. It is important to uphold this differentiation between intermediary and publisher because it would be impractical and unfair if liability was imposed on these third parties for user generated content. To combat these challenges, safe harbour provisions were designed to make sure that equitable accountability and necessary protection is provided to the intermediaries, over time, these provisions have evolved to incorporate obligations to remove unlawful content and due diligence requirements.

In India, this protection was provided through safe harbour provision. Section 79 of the IT Act[12] governs safe harbour provisions. Under this provision intermediaries won't be liable for third party content and they are granted immunity from liability, subject to certain conditions. Conditions such as they should act like a neutral platform[13], they should remove harmful content upon receiving actual information or government orders, they should not be responsible for the initiation of the transmission, should not select the receiver and should

[10] Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books 1999).
[11] Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books 1999).
[12] Information Technology Act, 2000, § 79.
[13] Christian Louboutin SAS v Nakul Bajaj AIRONLINE 2018 DEL 1962.

exercise due diligence[14]. Further obligations are imposed on the intermediaries by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 such as ensuring transparency in content moderation, exercising due diligence, removing unlawful content within specified timeframes and appointing grievance officers[15]. Accountability is enhanced by these provisions along with preservation of the benefits of safe harbour protections. In essence, a "safe harbour" or a safe haven is provided to intermediaries subject to the condition that they comply with certain requirements.

Judicial decisions have clarified the scope of intermediary liability. In the case of Shreya Singhal V. Union of India[16]The decision of the Supreme Court strengthened free speech, but also created challenges regarding enforcement in the process. The apex court limited the liability of intermediaries by creating a requirement for "actual knowledge" through legal orders. It was held by the Supreme Court that alleged content is required to be removed by the intermediaries only after they receive "actual knowledge" through a government notification or court order. This interpretation is important in order to prevent arbitrary censorship. However, it has received criticism as the platforms may delay action until formal notice is received and this creates enforcement challenges.

On the same lines, in the case of *MySpace Inc. v. Super Cassettes Industries Ltd*[17]., are not to be held liable of copyright infringement if they are not having actual knowledge of the specific infringement. It was held by the court that "notice and takedown" is the appropriate standard for digital intermediaries rather than pre-screening.

In the case of *Kent RO Systems Ltd. v. Amit Kotak*[18], the responsibilities of an intermediary were highlighted. It was held that as per the IT rules, an intermediary shall take down the infringing content and also disable access to the site within thirty-six hours of receiving receipt of infringement. It was also held that an intermediary shall inform its users of its terms of users, privacy policy and user agreement that they shall not showcase or host any content infringing the copyright of any other person. Thus, there has been a continued attempt by the judiciary to strike a balance between flow of information and accountability of intermediaries.

[14] Information Technology Act, 2000, § 79.
[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[16] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[17] MySpace Inc. v. Super Cassettes Indus. Ltd., 2017 SCC OnLine Del 12137.
[18] Kent RO Sys. Ltd. v. Amit Kotak, 2017 SCC OnLine Del 7185.

Nevertheless, safe harbour protections are exploited by digital platforms through ways such as lack of transparency, selective moderation policies, algorithmic amplification of harmful material and delayed response to harmful content[19]. Through these practices, platforms avoid liability and benefits from user engagement. Safe harbour protections are not merely used as a shield but intermediaries also benefit from them by using them as a mechanism to avoid accountability. Several patterns of exploitation of safe harbour protections to evade liability have been observed. In essence, the intermediaries use certain loopholes to benefit from the safe harbour provisions.

Deliberate delays in content removal are reported frequently, harmful content can spread widely if platforms fail to act promptly and don't take action in the required time. Inconsistency in applying content moderation policies is often observed. These selective moderation practices have raised concerns regarding lack of transparency and bias. Platforms may also promote controversial or sensational content to increase user engagement, even if such content is harmful. This type of algorithmic amplification defeats the purpose of providing safe harbour protections. Apart from that, sometimes users are not provided reasonable justification for content retention or removal decisions, which highlights a lack of transparency in decision making processes. These practices make the entire safe harbour provision counter effective.

The Digital Services Act[20] in the European Union have introduced stricter obligations. Proactive measures are required to be taken by platforms to ensure transparency and address harmful content. This puts the liability on third party platforms to ensure effectiveness and responsibility. Opposed to this, Section 230 of the Communications Decency Act[21] in the United States provides broader immunity. However, debates are going on regarding reforms in this provision.

A comparison can be drawn from the EU's Digital Services Act[22], it imposes more stringent obligations on platforms such as proactive monitoring. On the other hand, broader immunity is provided by the US under Section 230. If compared to the Indian framework, it can be inferred that India's approach lies between these two extreme situations, but challenges in

[19] Tarleton Gillespie, Custodians of the Internet (Yale University Press 2018).
[20] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), 2022 O.J. (L 277) 1.
[21] Communications Decency Act § 230, 47 U.S.C. § 230 (2018).
[22] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), 2022 O.J. (L 277) 1.

enforcement still persist. In India, enforcement and implementation challenges remain, however, certain obligations have been introduced.

These enforcement challenges lead to regulatory challenges which include balancing regulation and free speech, ambiguity in legal standards and weak enforcement mechanisms. Ambiguities lead to uncertainty regarding the legal obligations of intermediaries. There are several challenges in the regulation of safe harbour protections which can further limit the effectiveness of regulations if combined with weak enforcement mechanisms. Adding to that, creating a balance between accountability and freedom of expression which is a fundamental right as guaranteed under Article 19(1)(a)[23] creates a complex issue. Free speech may be restricted by over regulation and harmful content may proliferate easily in case of under regulation.

DISCUSSION

It has been demonstrated by the analysis that safe harbour protection is essential but is also increasingly misused by digital platforms. Platforms benefit from this immunity without fulfilling the corresponding responsibilities entrusted with them. The gap between practical implications and legal provisions is a major issue. Enforcement is inconsistent even when laws have been strengthened. This creates an easy way for platforms to evade liability and exploit ambiguities.

We must also consider the role of economic incentives which are achieved by these platforms by evading accountability.[24] In order to prioritise user engagement and revenue generation, platforms often neglect regulatory objectives which may be at conflict with the user demand and revenue generated. Harmful content may be tolerated or even prompted as a result of this economic incentive these third parties try to get. They create a mechanism through which safe harbour provisions can be used as per their convenience, i.e., when it does not come in the way of revenue generation through harmful or unlawful content.

Several reforms are required to address these challenges. The obligation of intermediaries must be defined through clearer legal standards. Compliance should be ensured by strengthening enforcement mechanisms. Content moderation processes should also have

[23] The Constitution of India, 1950, Article 19(1)(a).
[24] Frank Pasquale, The Black Box Society (Harvard University Press 2015).

greater transparency to ensure fairness. To ensure that safe harbour protections are preserved and to prevent their misuse a balance approach must be adopted.

CONCLUSION

A crucial role has been played by the safe harbour protections in the development of the digital ecosystem. These provisions have facilitated the free flow of information and enabled innovation by limiting intermediary liability. However, an increased misuse has been demonstrated by the digital platforms using these protections. Conflicting incentives, weak enforcement and ambiguous legal standards are some of the factors which have contributed to this problem. It has been shown by this paper that while India has taken significant steps in order to regulate intermediaries, still, challenges in accountability and implementation persist. This issue can be addressed by a more robust legal framework. To conclude, it is emphasised that a careful balance between safe harbour protections and need for accountability must be achieved. The intended purpose of this provision can be achieved by enhancing transparency, promoting responsible platform behaviour and strengthening enforcement.

Finally, it can be said that a pivotal role has been undeniably played by safe harbour protections in the development of the digital ecosystem and in facilitating the growth of this ecosystem. These provisions have enabled innovation, encouraged user participation and ensured the free flow of information. Safe harbour provisions must be recognised as essential for the functioning of the digital economy; however, their misuse poses a significant risk to legal accountability and public interest[25]. A nuanced and balanced approach which can preserve the benefits of these protections and also prevent their exploitation is required to ensure a transparent, accountable and fair digital environment.

[25] UN Human Rights Council, Report of the Special Rapporteur on Freedom of Expression (2016) A/HRC/32/38.