DEEPSTRAT

STRATEGY . POLICY . ACTION

INTERMEDIARY CLASSIFICATION AND LIABILITY

1.1. Research analysis – Intermediary Classification

Classification of Intermediaries under the proposed Digital India Act

Summary of Recommendations

1. Lay down definitions of key online intermediaries.
    - Align definitions under DIA with internationally accepted standard definitions.
2. **3 Models of Classification** to be considered in conjunction with each other for the DIA:

1. Classification based on technical functions

- Intermediaries operate across the Internet stack and their underlying technologies and business models are consequently different.
- This should the first level of classification.

2. Classification based on nature of services

- Helps tackle issues that arise from different types of online services.
- From the prism of user harms, 2 more factors are critical:

2.1 Use-cases and Risk Assessment

2.2 Network effects

3. Classification of new and emerging technologies

- Separate category to enable regulators, innovators and technologists to work together and build new frameworks.

Background

Nearly 23 years ago, when India passed the Information Technology Act, 2000, a 9.6 kbps connection used to cost INR 15,000 and the state-owned VSNL was the only internet service provider.[1]Today, India's median download speeds are 39.94 mbps (mobile) and 52.53 mbps (broadband).[2] It ranks 5th on the list of cheapest mobile data plans in the world and provides Internet access at an average cost of just INR 14 per GB.[3] In 2000, the Internet penetration in

[1] News18.com, India's First Internet Connection: VSNL's 1995 Plan Offered 40mins Per Day Usage at Rs 15,000, https://www.news18.com/news/tech/indias-first-internet-connection-vsnls-1995-plan-offered-40mins-per-day-usage-at-rs-15000-2780411.html , August 13, 2020.

[2] Speedtest Global Index, https://www.speedtest.net/global-index, accessed June 30, 2023

[3] Livemint, *Mobile data price in India among cheapest. Where it is less costly than India?*, https://www.livemint.com/technology/tech-news/mobile-data-price-in-india-among-cheapest-where-it-is-less-costly-than-india-11658991755978.html, July 28, 2022

India stood at 0.5% of its population[4]. Today, almost 50% of the Indian population is on the Internet.[5]

Clearly, today the Internet is the primary means that fuels innovation, commerce, communication, education and entertainment. These services are facilitated by intermediaries who make markets and societies work significantly more efficiently by "shortening the distance"[6]between users. Besides enabling India to become a trillion-dollar digital economy, intermediaries also make a significant contribution to innovation, social capital formation, freedom of expression, and better environmental outcomes, to name a few.[7]

The evolution of the Internet has resulted in intermediaries undergoing a sea change as well. For instance, when the IT Act was being drafted, the popular search engine Google had just been founded. Today, it is the most visited website on the Internet[8] and has expanded its services to email, video sharing, navigation, operating systems, cloud computing, artificial intelligence and many others.

When it comes to regulation of the slew of intermediaries present on the Internet and those that are emerging, a one-size-fits-all approach does not work. This is because these intermediaries are different from one another in terms of their technical and service-related functions and the impact that they have on society. Classification will help arrive at a regulatory model which protects user rights but at the same time, does not threaten the working of the Internet or impose disproportionate obligations on businesses.

The current approach

Just eight years into the enactment of the IT Act, we saw that there emerged a more nuanced understanding of the nature of intermediaries, the need for safe harbour, cybersecurity and critical information infrastructures in India. An amendment was brought about in 2008 which laid down a definition of intermediaries for the first time. This definition, which is still prevalent states, *"intermediaries with respect to any particular electronic records, means any*

---

[4] International Telecommunications Union, Percent Individuals Using Internet, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2022/December/PercentIndividualsUsingInternet.xlsx , accessed June 30, 2023

[5] Kemp Simon, Digital 2023: India, https://datareportal.com/reports/digital-2023-india , Datareportal, February 13, 2023

[6] Thelle, Sunesen, Basalisco, Sonne, Fredslund, Online Intermediaries Impact on the EU economy, file:///Users/Shachi_DS/Documents/DIA/Intermediary%20Classification/edima-online-intermediaries-eu-growth-engines.pdf, Copenhagen Economics, October 2015

[7] ibid

[8] Statista, *Most popular websites worldwide as of November 2022,* https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/, Accessed June 30, 2023

person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record"[9]

India's legal definition of intermediaries, which envisioned[10] telecom service providers, internet service providers, search-engines, online payment sites, online-auction sites, online-market places and even cyber-cafes, is long due for an overhaul. The Government of India's proposal to replace the IT Act with an overarching framework called the Digital India Act (DIA) is, therefore, an opportunity to redefine intermediaries and make them future-proof.

The DIA is not only going to bridge the technology-policy gap but is also aiming to be a futuristic legislation for the Indian digital economy. It is going to identify the current intermediary landscape of India and plan for new and emerging technologies such as Artificial Intelligence (AI). During two public consultations, the union Ministry of Electronics and Information Technology has presented that it will classify intermediaries into broad categories for better regulation. This paper looks at how this could be achieved, considering the underlying technologies, nature of services and use cases of online intermediaries currently and in the near future.

Suggested approach towards classification

Establishing definitional clarity

The DIA is an opportunity to lay down definitions of key online intermediaries. The Internet is a global common and works on certain internationally accepted principles and definitions. Jurisdictional approaches to defining intermediaries, therefore, do not align with the very nature of the Internet. The DIA should be leveraged to harmonise our definitions with the international standard. This can propel cross-border trade and catalyse India's goal of becoming a trillion-dollar digital economy by 2026.

Laying down definitions is an important first step towards classification. It brings about clarity for policy-makers about the various kinds of regulated intermediaries. According to Moore's law, computational capacity almost doubles every two years. Consequently, the nature and functions of intermediaries will always keep evolving. Delegated legislation or 'rule-making' can become a significant tool for building new definitions because it provides the advantage of easier updating. Once an intermediary is recognised through Rules and its regulation is tested through regulatory sandboxing, it can be included in the parent legislation through necessary amendments.

---

[9] S. 2(w), Information Technology Act, 2000, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[10] ibid

Classification Models

We recommend 3 models for classifying intermediaries. These models address the different aspects of intermediaries and have to work in conjunction with each other to arrive at a broad framework for classification under the DIA.

1. Classification based on technical functions

The Internet is "collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio."[11]

The Open System Interconnection model (OSI Model), developed by International Organisation for Standardisation depicts how information passes through seven layers when it travels from one computer to another. The spectrum is composed of the Application layer, which is closest to the user at one end, and the Physical layer, which is closest to the physical medium at the other.[12] The TCP/IP Model is more widely used. It consists of 4 layers, with the Application layer at one end and the Network access layer at the other.[13] Different engineering protocols apply at different layers of the internet but all the layers work collaboratively to transmit information from one end to the other.[14] The availability, reliability, and speed of the Internet, thus, depends upon effective functioning of these layers.

Online intermediaries operate across this Internet stack and their underlying technologies and business models are consequently different. In India, and other jurisdictions, intermediaries on different layers of the Internet have been presented with notices for content removal, summons for investigation and other law enforcement orders, irrespective of their role on the stack. Amicus briefs filed before the US Supreme Court in *Gonzalez v. Google*[15] have highlighted that uninformed laws can "cripple the technologies, operations, or investments that support a robust, free, and open Internet"[16].

---

[11] S. 1101(3)(C), The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §6501(6), https://www.govinfo.gov/content/pkg/PLAW-105publ277/pdf/PLAW-105publ277.pdf , Accessed June 30, 2023.
[12] Java T Point, OSI Model, https://www.javatpoint.com/osi-model, Accessed June 20, 2023.
[13] Cloudflare, What is the network layer? | Network vs. Internet layer, https://www.cloudflare.com/en-gb/learning/network-layer/what-is-the-network-layer/, accessed June 25, 2023.
[14] *Reynaldo Gonzalez, Et Al. V. Google LLC.*, 598 U. S. (2023), https://www.supremecourt.gov/opinions/22pdf/21-1333_6j7a.pdf
[15] ibid
[16] Brief for the US SC as Amicus Curiae, Internet Infrastructure Coalition; Cpanel, LLC; Identity Digital Inc.; Texas.Net, Inc.; And Tucows Inc., Gonzalez v. Google, https://www.supremecourt.gov/DocketPDF/21/21-

In India, there is a tendency to regulate intermediaries from a social media perspective. But all intermediaries cannot be regulated in the same manner and this is where the significance of classification comes in. Internet infrastructure companies that work on the Network layer (layer 3 of the OSI Model), such as those providing CDN or DDoS protection services do not have control content being posted on websites to which they provide services. If the law starts targeting them in such cases, it will not only put disproportionate obligations upon them but also threaten the efficiency and resiliency of the Internet.

New laws on intermediary regulation, such as the European Union's Digital Services Act (DSA), have established a legislative classification premised on the Internet stack and arrived at proportionate differential obligations for intermediaries. The DSA classifies online intermediaries into 3 broad categories[17]:

1. 'Mere conduit' services are involved in transmission (of information) in or access to a communication network.
2. 'Caching' services engage in automatic, intermediate, or temporary storage of information solely for the purpose of making transmission efficient.
3. 'Hosting' services undertake storage of information provided by their users.

Conduit and caching service providers do not face liability for merely transmitting or temporarily storing information, but hosting services providers can be held liable if they don't meet certain conditions laid down in the Act.

The underpinning of any legal classification in the DIA must be the well-established technical classification of the Internet stack. Once the law reflects the underlying technology and protocols governing the intermediary, regulation becomes easier and further categorisation can be made based on the specific legislative objectives.

2. Classification based on nature of services

The Internet layer which is closest in proximity to the end user is the Application layer. This layer and its protocols support building of 'digital platforms'.

The Organisation for Economic Co-Operation and Development, World Trade Organisation and International Monetary Fund have provided provisional guidance that digital platforms may be classified on the basis of the activity intermediated by them, i.e., the services they provide.[18] Intermediaries provide a host of services on the Internet, such as user-to-user

1333/252467/20230118141433052_2023%2001%2018%20i2C%20Amicus%20Brief%20-%20Bridges.pdf

[17] Article 2(f) "Intermediary Service", *Digital Services Act, 2022*, https://digitalservicesact.cc/dsa/art2.html

[18] Stahl, F., Schomm, F., Vossen, G. et al. A classification framework for data marketplaces, Vietnam J Comput Sci 3, 137–143 (2016). https://doi.org/10.1007/s40595-016-0064-2

messaging, social media, education, advertising, gaming and so on and so forth. This categorisation would enable the DIA to regulate platforms from the prism of user harm.

Some argue that two-sided platforms which link two user groups may be relatively easy to classify, but it may be difficult to pigeon-hole multi-sided platforms. Multi-sided platforms bring together more than two types of participants[19], for instance, giant social media platforms bringing together not only users but also game developers, ad-tech companies, payment gateways, etc.[20]

The nature of platforms will continue to get more diverse as they grow and add more service offerings. Yet, this is not a hard problem while arriving at a broad classification. From a regulatory standpoint, intermediary classification helps identify broad categories, but they will always be subject to multiple regulations. In the above example of giant social media companies, gaming, advertising, financial and other sectoral regulations will co-exist. The advantage of broad classification is in streamlining the functions of multiple regulators by clarifying the nature of regulated entities.

Classification helps in adoption of a graded-accountability approach based on the impact of intermediaries on users. This analysis can emerge from a study of two key factors – use cases and network effects.

1. Use-cases and Risk Assessment

For legislation which seeks to regulate intermediaries from the lens of user harms, a study of use cases and resultant risks will be useful. For instance, a meetings platform and a personal messaging service are both communication tools. But one has limited use for business meetings while the other facilitates messaging to a large audience. The former poses business or economic risks while the latter poses social or democratic risks. The potential for harms is vastly different and therefore, the impact has to be assessed differently.

The United Kingdom's Online Safety Bill takes a risks-based approach where the regulated entities are required to self-assess their risks and implement proportionate mitigation measures. Australia has adopted a co-regulatory[21] approach, where the industry develops a code of practice, in consultation with the Commissioner and that is made binding through legislation.

India is already looking at regulating some intermediaries such as online gaming platforms through the aid of Self-Regulatory Bodies. These bodies are going to conduct risk-assessments and develop standards for self-regulation that not only adhere to the law but are attuned to

[19] OECD, Rethinking Antitrust Tools for Multi-Sided Platforms, 2018, www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.html
[20] ibid
[21] Australia's Online Safety Act 2021, https://www.legislation.gov.au/Details/C2021A00076

industry risks. A similar model where industry led risk-assessments form the basis of regulation can prove to be dynamic yet effective, especially for new and emerging tech.

2. Network Effects

'Network effect' denotes the direct correlation between value of a platform and the number of its users.[22] A key driver of value-creation, and therefore impact of online platforms is the strength of their user-base.

Service-classification should, therefore, factor in network effects[23] of intermediaries. Large intermediaries have a heightened risk of harm because of their reach to a larger audience. A sub-classification on this ground enables attaching proportionately higher accountability to such intermediaries.

At present, India's IT Rules, 2021 categorise social media intermediaries with more than 5,000,000 users as significant social media intermediaries and they are mandated to meet additional due diligence requirements under Rule 4. Network effects would make the current threshold outdated pretty quickly.

The European Commission, on the other hand, has established a formula for declaring intermediaries as "very large". Any intermediary with a user-base of more than 10% of EU's population has to meet additional obligations. India would benefit from prescribing a formula for categorisation of significant intermediaries basis a demographic impact analysis.

3. Classification of new and emerging technologies

The advent of LLMs pose a fresh and possibly a fundamental challenge to how intermediaries are classified. It has been argued how users approached the internet through intermediaries was also based on the services they offered.[24] For instance, web directories and search engines were the intermediaries that helped structure the information available and lead users to them. However, LLMs are now scraping the web and developing the AI engine that

---

[22] Stobierski Tim, *What are Network Effects?,* https://online.hbs.edu/blog/post/what-are-network-effects, November 12, 2020.

[23] Ibid According to Stobierski, network effects have been seen to play out in 3 forms:

A. Direct network effect occurs due to an increase in the same user group. Social media companies have seen to benefit from this as friends of friends join their network.

B. Indirect network effect arises due to increase in users of another user group, such as increase in value of a social media company due to advertising.

C. Data network effect leverages greater data for greater value to the platform.

[24] Jain Sanjay, *ChatGPT: The Web will Change*!, https://deepstrat.in/2023/02/09/legal-and-technological-challenges-with-chatgpt/, February 9, 2023.

can provide answers. This immediately makes search engines redundant, a fact that big technology companies have recognised. Hence, Microsoft's Edge now offers a version of ChatGPT while Google has Bard. While ChatGPT's engine has data up to 2021, Bard offers additional capability to continue scraping the web.

The impact of this change will be significant. Not only does this change affect how users will access information, it will also start changing how information is structured, as well as how information is monetised. A combination of just these three aspects - access, structure and monetisation - will impact intermediaries so profoundly that it will need additional classification both at the technical as well as services level. Therefore, new and emerging technologies need to exist as a separate category of classification to enable regulators, innovators and technologists to work together and build new frameworks.

Conclusion

We have seen how the Internet has transformed since the time the IT Act was enacted and how it continues to evolve. The DIA, which aims to provide an open and safe Internet to the Indian users, must establish definitions and classifications of regulated online intermediaries. This exercise should be in tune with internationally accepted technical standard definitions. Using that framework, a nuanced service-categorisation can be evolved specific to the Indian context, keeping in mind its demographic, use-cases of intermediary services and the associated risks. Getting the classification right will not only safeguard users against online harms, but also enable ease of doing business, promote innovation and catalyse economic growth to help India achieve its goal of becoming a one-trillion-dollar digital economy.

Annexure – Illustrative table on the Intermediary landscape of India (Working draft)

Types of Intermediary	Technical Classification	Examples	Illustrative Harms
Online Marketplaces	Built on top of Application layer	Flipkart, Myntra or Amazon	Collection and processing of personal and non-personal data, dynamic pricing, or distribution of counterfeit goods
Mobile Ecosystems and Application Distribution Platforms	Built on top of Application layer	Android and iOS, and Google Play and App Store	Anti-competitive practices or listing fraudulent apps

Internet Search Services	Built on top of Application layer	Google, Yahoo or DuckDuckGo	Search neutrality, algorithmic biases, control over information landscape or collection and use of data
Social Media Intermediaries	Built on top of Application layer	YouTube, Instagram, Twitter	Hosting of illegal content, copyright infringements, or spread of misinformation and disinformation
Online Gaming Intermediaries	Built on top of Application layer	Dream11, Mobile Premier League	Addiction, financial losses, or self-harm
Cloud Service Providers	Across the Internet Stack	AWS, Google Cloud or Azure	Data resiliency, disaster recovery, or vendor-lock in
Artificial Intelligence	-	ChatGPT, Bard or Dall-E	Algorithmic biases, spread of misinformation, copyright issues, or educational risks
Ad-Tech Intermediaries	Built on top of Application layer	Criteo, Integrate or Ogury	Algorithmic biases, competition disadvantage, or risks to user privacy
Digital Media Intermediaries	Built on top of Application layer	Spotify, Audible or online news websites	Spread of false information, or obscenity
Internet Infrastructure Intermediaries	Network layer	Cloudflare, Akamai or NordVPN	Malware, spoofing, DDoS attacks

1.2. Research analysis – Tackling Intermediary Liability

Summary of Recommendations

1. Define and clarify who and what is to be regulated.
2. Develop a clear classification scheme for intermediaries. Any classification must consider the functions of the intermediaries, as well as the size of their user base. A clear scheme with objective thresholds for classification will ensure regulatory clarity and proportionate due diligence obligations.
3. Remove general content monitoring obligations currently in force, to protect the constitutional right to free speech on digital platforms. If general monitoring obligations are imposed, they must be in line with principles, such as the Manila or Santa Clara Principles that have been formulated with the help of multiple stakeholders, including India.
4. Since intermediaries are required to take down infringing content upon receiving knowledge of its existence, clear criterion must be established for reports, requests, and orders from individuals or entities so that a standard for establishing "actual knowledge" can be determined.
5. Institute a conditional liability framework with penalties that are civil or monetary in nature. Exclusion from safe-harbour should not be a penalty imposed on platforms, unless there is evidence of repeated non-compliance.
6. Establish an appeals process for platforms to demand more transparency on take-down notices from the government.
7. Evolving/improving technology to address intractable issues pertaining to content, privacy, and security is important. Such improvements must be in line with principles like privacy/security by design or judicial oversight.

Executive Summary

India's digital economy is at the precipice of massive change. The Digital India Act, which is set to replace the Information Technology Act 2000, will govern India's digital landscape for the coming decade. It provides the opportunity to create a law that is forward-looking, fosters innovation, and creates a safe and trusted internet for users. To that end, the DIA must provide its digital actors with regulatory and legal clarity, proportionate obligations, and transparency enhancing measures. Furthermore, it must develop a framework to effectively enforce its regulations and provide adequate appellate mechanisms. This is an opportunity for India to develop a model where the government and private enterprises share responsibility for the well-being of users, so that we can collaboratively attain India's dream of becoming a trillion-dollar economy by 2026.

What is intermediary liability?

At a recent public consultation for the Digital India Act (DIA), the Minister of State for Electronics and Information Technology, Mr. Rajeev Chandrashekhar raised a provocative question. He asked participants if the current safe harbour provision under the Information Technology Act, 2000, could be removed. For more than two decades, the safe harbour

provision has given platforms, commonly known as intermediaries who host user generated content, to offer services without having to face consequences of what their users do with it. This allowed intermediaries to safely innovate platforms without the risk of legal threats and costs due to user behaviour.

As the internet and internet-enabled businesses grew, we began to see a surfeit of unanticipated online risks and harms such as misusing social media platforms to spread misinformation and disinformation or worse, even target vulnerable groups like women. For intermediaries running these platforms, it is a question of whether they can be held liable for what their users do. If so, then what is the degree of their liability and on what basis can it be determined?

Why is intermediary liability a complex problem?

As the conversation around intermediary liability becomes more evolved in India, the government must balance attaching liability to platforms while also not undermining their businesses. The government as an elected body also has a responsibility towards its citizens and sees intermediary liability as a tool for preventing online harm. Additionally, the government is often a user of platforms itself and will directly be impacted by any regulation it imposes. This means that a complex interplay of interests must be navigated to prevent user harm and the growing economic and social influence of intermediaries from going unchecked from the anti-competitive and market-distortion point of view.

If the government decides to ask platforms to adjudicate user-to-user grievances, it will have to provide intermediaries with clarity about what behaviours and actions constitute user harm. Any attempt to define user harm, therefore, has to avoid imposing disproportionate compliance burden on intermediaries while also protecting users to the maximum extent from other users that misuse or weaponise platforms in a plethora of ways.

How has intermediary liability taken form in India?

In India, intermediaries are regulated under the Information Technology Act,2000 which defines them as any person who "on behalf of another person receives, stores, or transmits (…) or provides any service with respect to an electronic record." [25] This broad definition covers intermediaries who provide physical infrastructure services that make internet access.

possible (such as Internet Service Providers, Telecom Service Providers), and platforms like Twitter and Flipkart that host content created or shared by users for social, commercial, and other purposes. Intermediaries are treated as separate from publishers who curate online content[26], which is crucial for them to claim exemption from liability since they profess to not have similar editorial control over the content[i] they host.

[25] The Information Technology Act, 2000. S 2(1)(w).

[26] PRS Legislative Research. 2021. "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021" https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines- and-digital-media-ethics-code-rules-2021

Usually, governments employ a classification scheme to identify categories of platforms based on their function, service, or reach in order to determine the extent of their liability. However, India lacks such a classification scheme and only classifies intermediaries as social media intermediaries, significant social media intermediaries (SSMIs), or online gaming intermediaries.

Social media intermediaries are defined as those intermediaries who "primarily or solely enable(s) online interaction between two or more users and allow(s) them to create, upload, share, disseminate, modify or access information using its services." Those social media intermediaries having a number of registered users that meet or exceed the threshold notified by MeitY are called SSMIs. Notably, in India, courts play a significant role in determining whether an entity can be called an intermediary and can avail safe harbour provided by Section 79 of the IT Act.[27] Safe harbour refers to the exemption of liability and promotes trade, commerce and innovation by not holding intermediaries accountable for the content hosted by them if they do not have direct control over it.

It is also worth looking at how other jurisdictions have evolved their intermediary liability framework. In the EU, the Digital Services Act (DSA) identifies intermediaries based solely on the technical services/functions they provide as; 'mere conduit', 'caching' and 'hosting' services. To impose proportionate due diligence obligations, it creates further categories within intermediary services. Therefore, hosting services are further identified as online platforms, and within that category, as very large online platforms (VLOPs), based on the size of their user base. This pyramidic approach of obligations partly matches the intent of Indian legislation which also imposes greater obligations on significant social media intermediaries and online gaming intermediaries.

The UK's Online Safety Bill (OSB)[28] is a framework based on risk-assessment and mitigation[4]. Its approach to allocating risk is informed by the exercise of exhaustively and descriptively defining various services and content such as user-to-user services, search services, combined services, and user-to-user content. It uses these definitions to identify what is to be regulated content and defines service providers who provide access to regulated content. Following this, it arrives at a definition for regulated service providers, which it identifies as user-to-user service providers and search engine service providers. It also regulates some intermediaries who act as pornographic content providers. This contrasts with India, which instead only defines the services and providers being brought into the regulatory ambit, as and when it decides to regulate them. OSB's approach lends better regulatory clarity through definitional exactitude.

How are due diligence obligations imposed in India and abroad?

[27]Devadasan, V., 2023. Report on Intermediary Liability in India (December 2022). *Centre for Communication Governance*.

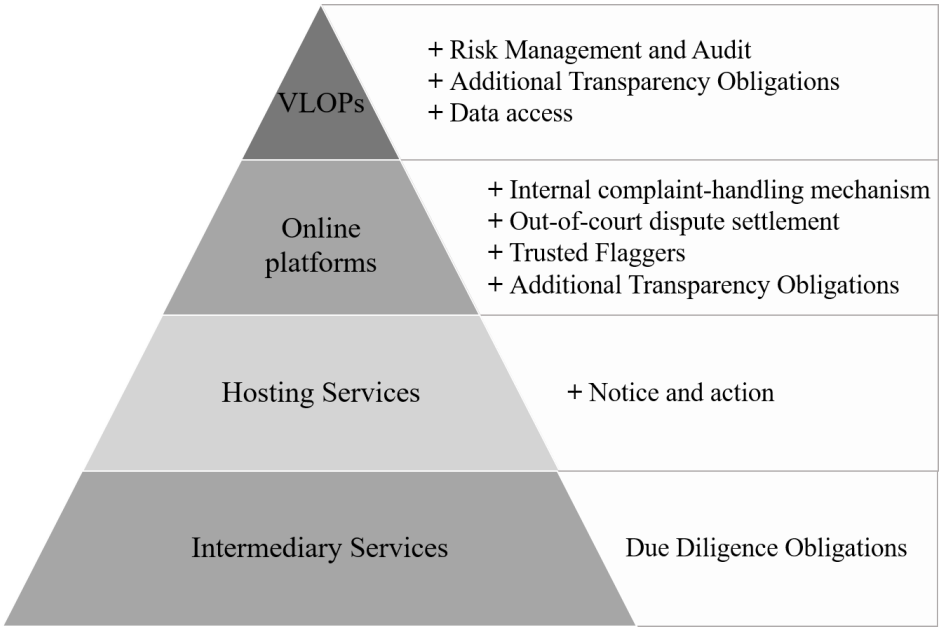
[28] Woods, L. 2022. The UK Online Safety Bill: an outline. https://blogs.lse.ac.uk/medialse/2022/03/25/the-uk- online-safety-bill-an-outline/

Due diligence obligations outline rules intermediaries must comply with and are a pre-emptive tool for the government to protect users from harm. Liability exception or safe harbour is provided on the condition that intermediaries adhere to these rules and procedures. This is called conditional liability. In India, due diligence obligations for all intermediaries are detailed in Rule 3 of the IT Rules 2021. The due diligence obligations are two-tiered, with Rule 4 specifying additional due diligence obligations pertaining to prohibited content for SSMIs and online gaming platforms.

India's approach resembles that of the DSA and OSB which also follow a conditional liability framework, but differs with regards to procedures, requirements, and the extent of obligations that platforms are subject to. The DSA, for instance, also imposes "tailored asymmetrical obligations" on intermediaries based on their classification, wherein some categories of intermediaries are subjected to additional obligations. The most general and baseline condition to be exempt from liability is that the service provider in no way intervenes with the transmission, storage or provision of access to illegal content. However, no general monitoring obligations lie on intermediaries as a core principle of the DSA.

The DSA further lists the specific conditions to be complied with for each service category. For instance, VLOPs, which are defined as having an average of 45 million monthly users,[29] have the highest number of conditions to meet. In addition to obligations that other categories are subject to, VLOPs must take risk management, audit, transparency, and data access measures. Providers of intermediary services cannot be held liable for any illegal information they transmit, store or provide access to, if they meet the general and category-specific obligations. Enforcement of these obligations follows a supervised risk management approach, with coordinators to oversee implementation and communication between the intermediaries and the executive.

[29] European Commission. N.d. Europe fit for the Digital Age: new online rules for platforms. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital- services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_en#tailored-asymmetric-obligations



Source: Buiten, M.C., 2021. The Digital Services Act From Intermediary Liability to Platform Regulation

The UK's OSB also takes a similar approach, with the stated aim of imposing differentiated and proportionate obligations. Importantly, the UK does not necessarily require that platform services be able to stop all instances of harmful content or assess every item of content for their potential to cause harm. The duties on platforms are limited by what is proportionate and technically feasible. All providers of regulated user-to-user and search services have duties of care pertaining to illegal content and their risk assessment.

They further have duties pertaining to content reporting and complaints procedures, and responsibilities pertaining to freedom of speech and privacy. All providers of services that are likely to be accessed by children also must conduct children's risk-based assessments and take steps to protect children's online safety. (Such a risk-based approach and identification of protected stakeholders is missing in India, which is yet to attain definitional clarity.) For the sake of proportionality and feasibility, some regulated service providers are classified as Category 1, Category 2A, or Category 2B because their services are estimated to involve higher risks for users.[30] Entities belonging to these categories are subject to additional but proportionate diligence requirements, which can be summarised through the following table:

[30] Nuthi, K. and Tesfazgi, M. 2022. Reforming the Online Safety Bill to Protect Legal Free Expression and Anonymity. https://www2.datainnovation.org/2022-uk-online-safety-bill.pdf

Table 1: Types of Content and Services Regulated by the Online Safety Bill

	Category 1	Category 2A	Category 2B
Definition	Higher-Risk User-to-User Services	Search Engines	Lower-Risk User-to-User Services
Duties for Illegal Content	Covered	Covered	Covered
Duties for Content That is Legal But Harmful (Children)	Covered	Covered	Covered
Duties for Content That is Legal But Harmful (Adults)	Covered		
Duties to Protect Content of Democratic Importance	Covered		
Duties to Protect Journalistic Content	Covered		
Duties to Prevent Fraudulent Advertising	Covered	Covered	

Source: Nuthi, K. and Tesfazgi, M. 2022. Reforming the Online Safety Bill to Protect Legal Free Expression and Anonymity

Intermediary Liability and Safe Harbour

Notably, the ability of SSM intermediaries and platforms to act against prohibited content is contingent on them having "actual knowledge" of such activity. Actual knowledge is when platforms can demonstrate that they possess necessary information to identify, assess, and take action against content that is legally prohibited or suspect. It can be achieved through notices issued privately by users or through takedown notices ordered by the government or a court.

The 2011 IT Rules instituted a notice-and-takedown regime in India, which prohibited platforms from knowingly hosting prohibited content once they received a written complaint. However, with the Shreya Singhal v. Union of India judgement in 2015,[31] courts established that intermediary would be liable and susceptible to safe harbour denial only if it failed to take down content upon receiving a reasoned order by the government or a court. However, subsequent iterations of the IT Rules continue to require that platforms receive and act on private complaints at the risk of losing safe harbour. Furthermore, the 2022 IT Rules broadened the scope of actual knowledge by requiring intermediaries to proactively prevent the hosting of content that can cause user harm, rather than simply relying on notices from users, the government or courts.

[31] *Shreya Singhal vs. Union of India* (2015) 5 SCC 1

The DSA requires intermediaries to promptly remove or disable access to illegal content upon awareness, while respecting the principle of freedom of expression, to qualify for liability exemption. To establish actual knowledge, notices must contain specified information that enables the intermediary to reasonably identify, assess, and take appropriate action against the allegedly illegal content.[32] Non-compliance with the DSA does not result in loss of safe harbour, but rather a graded response, such as imposition of fines and periodic payments, which in the most severe cases, can amount to up to 6% of their annual turnover. The DSA further provides safeguards against penalties and fines and gives platforms the right to be heard and access to the relevant files, records, and publications pertaining to decisions that impose liability.

In the UK, platforms must demonstrate to the regulator that their processes are effective in preventing harm. Failure to meet the requirements of the Bill will result in a fine of up to £18 million or 10 percent of annual global turnover, whichever is greater. Criminal action will be taken against senior managers who fail to comply with information requests pertaining to prohibited activities and instances. In the most extreme cases, and only upon agreement of the courts, payment providers, advertisers and internet service providers may be required to stop working with a site, preventing it from generating money or being accessed from the UK.[33]

Much like the EU, redress for platform finds mention in the OSB itself, allowing platforms to appeal against the regulator's actions or notices. While India does have procedures for enforcing due diligence obligations, platforms do not have similar or sufficient redress mechanisms to challenge or seek more information on takedown orders. The absence of such safeguards can force intermediaries to take action against lawful content, especially under the current liability regime where the penalty is the loss of safe harbour under Section 79 of the IT Act, 2000. As is evident above, the EU and UK rely more on monetary penalties to enforce adherence to obligations, with loss of safe-harbour being an extreme and last resort tool.

What are some complex issues that intermediary liability raises?

The requirement to proactively identify content that may be unlawful can lead to platforms monitoring and excessively removing user content to avoid liability or the loss of safe harbour. Moreover, platforms do not have the necessary skills, definitional clarity, or the authority to determine the legality of content, a decision which can only be exercised by courts. Furthermore, any decision it makes will have a significant impact on all users. The narrow focus on intermediary liability has also distracted India from seriously considering other mechanisms to counter user harm that are more bottom-up, such as user empowerment.
General monitoring obligations are categorically avoided by the DSA as well as its e-

[32] Buiten, M.C., 2021. The Digital Services Act From Intermediary Liability to Platform Regulation. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *12*, p.361.

[33] Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport. 2022. A guide to the online safety bill. https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill#how- the-bill-will-be-enforced

Commerce Directive. Furthermore, the DSA also provides safeguards to platforms against penalties and fines imposed by the government, such as the right to be heard and to access files and publications of decisions. A similar provision is available in the OSB, which also allows platforms to appeal against the regulator's notices and, where relevant, penalties.

How can we navigate intermediary liability?

Good law making, capable enforcement mechanisms and fair appellate forums would be the key to navigating intermediary liability. Any approach to regulating platforms should approach the issue of user harm from a shared responsibility perspective. It also must undergo rigorous consultations in a transparent fashion. Furthermore, they must be based on data and evidence-based research and consider best practices of other jurisdictions' regulatory frameworks. To that end, the following recommendations may be considered:

1. Define and clarify who and what is to be regulated.
2. Develop a clear classification scheme for intermediaries. Any classification must consider the functions of the intermediaries, as well as the size of their user base. A clear scheme with objective thresholds for classification will ensure regulatory clarity and proportionate due diligence obligations.
3. To protect the constitutionally protected freedom of speech on digital platforms, general content monitoring obligations must be removed. If general monitoring obligations are imposed, they must be in line with principles that have been formulated with the help of multiple stakeholders, including India.
4. Since intermediaries are required to take down infringing content upon receiving knowledge of its existence, clear criterion must be established for reports, requests, and orders from individuals or entities so that a standard for establishing "actual knowledge" can be determined.
5. Institute a conditional liability framework with penalties that are civil or monetary in nature. Exclusion from safe-harbour should not be a penalty imposed on platforms, unless there is evidence of repeated non-compliance.
6. Establish an appeals process for platforms to demand more transparency on take-down notices.
7. Evolving/improving technology to address intractable issues pertaining to content, privacy, and security is important. Such improvements must be in line with principles like privacy by design or security by design.

1.3. Research analysis - Tackling Safe Harbour Through the Digital India Act

Safe Harbour

It has famously been said that twenty-six words shaped the internet when, in 1996, USA added Section 230 to its Communications Decency Act[34]. With this provision, digital platforms and intermediaries in the United States could no longer be held liable for content generated by its users. This "safe harbour" prevented intermediaries from incurring undue legal costs, and from diluting freedom of speech by proactively monitoring their platforms for infringing content.

In India, safe harbour provisions have been outlined by Section 79A of the Information Technology (IT) Act. These were introduced in 2008, after the CEO of Bazee.com, Mr. Avnish Bajaj was imprisoned because of pornographic content that was circulating his platform[35]. Since, then the government's stance on safe harbour has shifted drastically. As India prepares to replace the Information Technology (IT) Act 2000 with the proposed Digital India Act, India has rashly announced that it is reconsidering its safe habrour provisions.

The sweeping pivot in public discourse is present even in the United States, which has thus far been the staunchest defender of legal immunity for digital intermediaries. However, this stance is now challenged by a sweeping change in public discourse. This reveals that people across jurisdictions can no longer dismiss that online harms have evolved, and new ones have emerged. This is evidenced by an increasing number of cases being heard by courts across the world, each grappling with one key question- when can intermediaries be held liable for hosting illegal content created by its users?

What is India's Safe Harbour approach?

Section 79A stipulates certain conditions intermediaries must fulfil to be immunized from legal responsibility, an approach commonly known as conditional liability. Its conditions can be summarised as its **3A approach** because it outlines obligations related to *action, awareness, and adherence.*

Firstly, intermediaries seeking safe harbour protection cannot play the active creative, curative, or editorial role that publishers play. *Secondly,* India holds intermediaries liable for third-party content if it can be demonstrated that the intermediary was aware of the illegal content it was hosting. To establish awareness, India adopts a notice-and-takedown approach wherein awareness is established through notices or orders issued by the government, or through personal notices received by users.

---

[34] https://www.cato.org/events/twenty-six-words-created-internet

[35] https://www.medianama.com/2019/12/223-avnish-bajaj-redux-supreme-court-of-india-denies-relief-to- google-in-criminal-defamation-proceedings/

Thirdly, in addition to remaining passive conduits of information, intermediaries must follow any guidelines notified by the Central government such as the IT (Amendment) Rules. The IT Rules are subordinate legislation and have been used extensively by the Centre since 2021 to reign in big digital players. While regulating large digital platforms is necessary to preserve the legal health of the internet, a reconsideration of safe harbour requires a careful evaluation of what that entails for two key stakeholders whose interests are intertwined- users and digital platforms.

What does loss of Safe Harbour look like?

On June 30, 2023, the Karnataka High Court decided to penalise Twitter with a large INR 5 million rupee fine[36]. The social media intermediary was held liable for non-compliance with 39 takedown orders issued by the Centre during the 2020 farmer's protests, under Section 69A. But the implications for Twitter and its users extends beyond a one-time fine. The judgement sets a dangerous precedent by setting aside the free-speech and procedural fairness issues raised by Twitter during the case. It is simultaneously signalling to digital intermediaries the legal costs that face them should they challenge the government's content moderation policies.

An average user has much to lose when platforms are held responsible for actions that are not their own. If a users' activities are viewed solely as potential legal costs, intermediaries like Twitter may be forced to engage in additional self-regulatory conduct to adhere to the law. This can mean pre-emptively clamping down on content which can be *interpreted* as illegal. The jeopardy this poses to the internet is massive because of the internet function as an equaliser of power, democratising access to information. Movements like #MeToo or Black Lives Matter may have never occurred, much less gained traction, had intermediaries intervened pre-emptively to avoid culpability in implicating powerful people.

A loss of safe harbour affects all different kinds of intermediaries, and consequently all different kinds of stakeholders. If an e-commerce giant like Amazon were to be held liable for copyright infringement, it could lead to a change in its entire business model. It may begin undertaking precautionary measures like verification, certification, or takedown to prevent liability costs[37]. But Amazon is a direct competitor of the very the businesses it provides a platform to, which are often much smaller and heavily reliant on its reach. Faced with higher costs, smaller businesses may be forced to remove their businesses from the platform, affecting not just consumers but the economy writ large.

The impact of safe harbour on the business models intermediaries employ cannot be separated from the costs that users will ultimately have to bear. As platform-based business models evolve, a safe harbour framework premised on protecting users and businesses cannot overlook the economic implications of holding platforms liable.

---

[36] https://www.medianama.com/2023/06/223-karnataka-hc-dismisses-twitters-petition/

[37] https://link.springer.com/article/10.1007/s10657-022-09728-7#:~:text=According%20to%20this%20regime%2C%20a,that%20would%20maximize%20social%20welfare.

No one-size fits all approach to penalties

Currently, we gauge liability based on an intermediary's awareness, adherence, and action. However, each of these three criteria are not always enforced in a manner that is proportionate or fair. It is undeniable that the tools platforms provide can be misused by ill-intentioned users. This is a fact well recognised by platforms who often go beyond the mandates of the law to act and prevent user harm. Meta, for instance, runs extensive operations to counter terrorist activities on Facebook[38]. Despite their best efforts, intermediaries cannot contain or monitor how their platform is used at all times. A user predisposed to addiction is biologically driven to abuse their time on social media or gaming platforms. It is untenable then to suggest that intermediaries be penalised for factors beyond their technical and feasible control.

Adherence, as demonstrated by Twitter's experience, can be difficult when the conditions for safe harbour are substantially and procedurally flawed. Demanding compliance with guidelines and conditions requires transparent enforcement by the government and sensitivity to the limitations platforms often operate under. This generates a demand for two things. One, India requires a framework that accurately captures different intermediaries' contribution to the digital ecosystem. Without a scientifically grounded classification scheme, India's approach to penalising online intermediaries will remain plagued with inevitable infirmities.

A sound classification scheme can help meet the second demand, which is that of graded penalties. Since intermediaries and their user bases are diverse, a uniform penalty will fail to capture the different risks and limitations inherent to an intermediary's services. India should consider a graded mechanism to penalty, as opposed to a loss of safe harbour. Monetary penalties can be the primary resort for the government to ensure compliance, the amount of which can be determined by an appellate or quasi-judicial authority. Loss of safe harbour, should it remain a consideration, should only be a last resort penalty after evidence of repeated non-compliance.

The condition of awareness is not without difficulties either. An intermediary can only be penalised when they can objectively be determined to have overlooked user harm. This is why India employed a notice-and-takedown approach under the IT Act. More recently, it has started demanding that intermediaries remain proactive in monitoring and identifying illegal content on their platforms[39]. However, this is unfeasible for most intermediaries and the compliance burdens it imposes can hinder younger platforms from scaling up. This can have cascading effects on free speech and privacy and hamper businesses' right to a fair and free market.

---

[38] https://www.brookings.edu/articles/dual-use-regulation-managing-hate-and-terrorism-online-before-and- after-section-230-reform/

[39] https://www.eff.org/deeplinks/2022/07/new-amendments-intermediary-rules-threaten-free-speech-india

Developing standards for awareness and appeals

Most progressive democracies equip their liability regimes with standards for information notices and orders. The EU[40] and UK[41] both require that intermediaries be provided with a standardised set of information that can help them identify, assess, and act against prohibited content. The EU's Digital Safety Act goes a step further by requiring that notices contain information about judicial redress available to recipients so they may challenge the notice or order.

Not only does no such standard exist in India, but the safeguards the IT Act and its Rules establish are often circumvented, hindering transparency. The Karnataka High Court's judgment demonstrated this by allowing the Centre to issue blocking orders without providing reasons to either the intermediary or the user. Blocking orders issued under Section 69A(1) follow a different procedure compared to any notices issued under Section 79(3)(b). The scope for redressal within this existing framework is very limited and can further deter transparency. Therefore, a standard operating procedure for such orders must be evolved so that procedural safeguards are better outlined within the law.

In the interest of fairness, the government should also consider issuing certain principles that intermediaries are required to follow while moderating content. The Santa Clara Principles for Accountability and Transparency in Content Moderation[42] offer a useful standard. Intermediaries who can demonstrate that the principles were followed in moderating or blocking content should not be held liable.

It is true that the government may occasionally be required to withhold information from the public to preserve security. That such a carve-out not be abused, however, remains a concern. To this end, India may consider making Section 79A proceedings public. This can allow for sufficient transparency without forcing the government to furnish information that can jeopardise public safety.

Another consideration for India, drawing from jurisdictions like EU and the UK, is that of remediation. The 2004 UN Guiding Principles on Business and Human Rights[43] stress that parties that have caused or contributed to harm should be made to cooperate in their remediation through legitimate and due process. In the case of safe harbour, such remediation can be offered by reinstating content that has been found to be legally valid. Furthermore, appeals processes for intermediaries to challenge or question content removal orders and notices should also be established by a forward-looking legislation like the DIA. Currently, the Grievance Appellate Committees (GACs) instituted by the IT Amendment Rules 2022 allow for users to appeal against platforms. However, no mechanism exists for platforms to appeal against the government outside of courts. The government should therefore deliberate on how and where such a mechanism can be accommodated. Whether the same

---

[40] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065

[41] https://publications.parliament.uk/pa/bills/cbill/58-03/0209/220209.pdf

[42] https://santaclaraprinciples.org/

[43] https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

can be provided within the existing GAC mechanism should be an open question that the government engages in during the ongoing consultations for the Digital India Act.

Conclusion

Though the internet is greater than the sum of its parts, its countenance cannot be divorced from cases of its use and misuse. The dilemma then facing regulators is how and when to begin holding platforms liable for their users' behaviour. Digital marketplaces and sites are diverse and widely adopted, which is why any calibration of liability can have a myriad of spillover effects. Increased compliance or legal costs can trigger a shift in business models, which will in turn have an avalanche effect on everything from competition and innovation to free speech and democracy. As India's stance dangerously veers against safe harbour, the need for transparency, proportionality, and risk considerations in digital regulation is starker than ever.

1.4. Principles for Intermediary Liability and Classification

1. **Necessary, proportionate and differential obligations**

1.1. Regulatory requirements for digital platforms should be tailored to their:

1.1.1 size,

1.1.2 functionality,

1.1.3 technical service,

1.1.4 risk profile, and

1.1.5 user-base size.

1.2 Proportionate obligations ensure that the due diligence required of platforms are feasible and executable. (*Explanation: Differential regulatory requirements also protect smaller companies from facing undue compliance burdens that can stifle their growth*.)

1.3 The principle of necessity will create a reasonable correlation between liabilities and objectives of the Act. (*Explanation: This is a key tenet of necessity established in the Supreme Court judgment of Justice K. S. Puttaswamy & Anr. vs. Union of India & Ors., 2017)*

2. **Principle of shared responsibility**

2.1 The prevention of user harm is a shared responsibility between the government and intermediaries.

2.2 Must adhere to the fundamental rights established under Article 19(1) of the Constitution.

2.3 Internet intermediaries must encode human rights independently from states while following the rule of law and offering effective safeguards and remedial opportunities to their users. *(Explanation: This has been enshrined in the UN Guiding Principles on Business and Human Rights)*

3. **Conditional Liability for Third-Party Content**

3.1 Adopt a conditional liability framework instead of strict liability for third-party content hosted on platforms.

3.2 Liability should be determined on a case-by-case basis by courts.

3.3 Principle of safe harbour: Legal immunity should exist where intermediary has not been involved in the modification of content.

4. Curb General Content Monitoring Obligations

4.1 Intermediaries should not be required to proactively monitor user-generated content. (*Explanation: This principle finds mention in the EU's recent Digital Services Act, the predecessor of which guided India's intermediary liability framework.)*

4.2 Any content monitoring obligations should be in line with relevant and established principle-based frameworks such as the Santa Clara Principles on Transparency and Accountability in Content Moderation which emphasise*:*

4.2.1 Human Rights and Due Process

4.2.2 Easy-to-Understand Rules and Policies

4.2.3 Sensitivity to Cultural Context

4.2.4 Transparency to the User

4.2.5 Integrity and Explainability

5. Risk Mitigation:

5.1 No liability on intermediaries for failing to prevent all instances of unlawful content hosted by them.

5.2 Intermediary liability should be assessed based on the risk mitigation measures adopted by them to protect users.

6. Transparency and Accountability

6.1 Transparency can be ensured if the government publishes in clear and accessible formats:

6.1.1 legislation and policies on intermediary liability,

6.1.2. transparency reports of all content takedown and restrictions.

(*Explanation: This is stated by Principle 6 of the Manila Principles, which have been developed collaboratively with stakeholders, governments, and civil society actors from across the world, including India)*

6.2 Transparency can also be achieved by establishing:

6.2.1 Due process for content removal. Orders must contain certain items of information that establish:

6.2.1.1 the legal basis for content removal,

6.2.1.2 the period for within which the content must be removed,

6.2.1.3 the duration for making content unavailable,

6.2.1.4 contact details of the issuing party, and

6.2.1.5 the judicial redress avenues available to intermediaries and users to challenge notices or orders.

(*Explanation: Principle 3 of the Manila Principles states that requests for content removal must be clear, unambiguous, and follow procedures and safeguards established by law.)*

6.2.2 Review and reinstating mechanisms. Intermediaries and users must be provided with the effective right to be heard if any content removal takes place.

6.2.2.1 Mechanisms must be provided to review and appeal content removal decisions.

6.2.2.2. Any piece of information that is found to be legally valid upon review should be reinstated, and mechanisms for its reinstatement ought to be in place.

6.2.3 Remediation. Intermediaries and users must be provided with effective grievance redressal mechanisms to challenge takedown orders issued by the government.

(Explanation: In accordance with the UN's Guiding Principles on Business and Human Rights, parties that have caused or contributed to harm should be made to cooperate in their remediation through legitimate and due process)

7. Proportionate Sanctions

7.1 Any sanction imposed by the legislation on intermediaries must meet the test of proportionality by considering the context of an intermediary's involvement and limitations in preventing user harm.

7.2 Loss of legal immunity is a disproportionate sanction to uniformly impose on all intermediaries.

7.3 The intermediary liability regime must be enforced through monetary and civil penalties.

---

[i] PRS Legislative Research. 2021. "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021" https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines- and-digital-media-ethics-code-rules-2021